Proficy* Historian

GETTING STARTED WITH HISTORIAN

Version 5.5

June 2013

All rights reserved. No part of this publication may be reproduced in any form or by any electronic or mechanical means, including photocopying and recording, without permission in writing from GE Intelligent Platforms, Inc.

Disclaimer of Warranties and Liability

The information contained in this manual is believed to be accurate and reliable. However, GE Intelligent Platforms, Inc. assumes no responsibilities for any errors, omissions or inaccuracies whatsoever. Without limiting the foregoing, GE Intelligent Platforms, Inc. disclaims any and all warranties, expressed or implied, including the warranty of merchantability and fitness for a particular purpose, with respect to the information contained in this manual and the equipment or software described herein. The entire risk as to the quality and performance of such information, equipment and software, is upon the buyer or user. GE Intelligent Platforms, Inc. shall not be liable for any damages, including special or consequential damages, arising out of the user of such information, equipment and software, even if GE Intelligent Platforms, Inc. has been advised in advance of the possibility of such damages. The user of the information contained in the manual and the software described herein is subject to the GE Intelligent Platforms, Inc. standard license agreement, which must be executed by the buyer or user before the use of such information, equipment or software.

Notice

©2013 GE Intelligent Platforms, Inc. All rights reserved. *Trademark of GE Intelligent Platforms, Inc.

Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries.

All other brands or names are property of their respective holders.

We want to hear from you. If you have comments, questions, or suggestions about our documentation, send them to the following email address:

doc@ge.com

Table of Contents

Getting Started with Historian 1

Reference Documents 1

What's New in Historian 5.5 2

Multi Field User Defined Data Types 2

Dynamically Sized Array Tags 2

Enhanced Data Query Filtering 2

Updated Operating System Support 2

Permanent Rename and Permanent Delete of Tags 2

New Calculation Modes 3

New Query Modifiers 3

New Comparison Modes 3

New Sampling Mode 4

Overview of Historian 4

System Components 7

Historian Alarms and Events 7

Historian Data Collectors 7

Historian File Collector 8

Historian Administrator 8

Historian Server 8

Excel Add-In 9

Historian OPC HDA Server 9
Historian User API 9
Historian SDK 9
Historian Client Access API 10
Historian Migration Tools 10
Understanding the System Architecture 10
iFIX Implementation Guidelines 11
Historian Alarm and Event Archiving 12
Setting up the Historian Environment 12
Task Overview 13
Hardware Requirements 13
Software Requirements 19
Compatibility with other Proficy Products 21
Supported Regional Settings 22
Time and Date Formatting 23
Supported Data Types 23
The Hardware Key 24
Installing the Hardware Key 25
Disabling Guest Accounts 25
Optimizing Virtual Memory 26
Using a Remote SQL Server to Store Alarms 26
Installing Historian Software 27

Installing the Historian Server 27
Log Files Created After You Start Historian for the First Time 30
Installing Historian Non-Web Administrator 30
Starting the Historian Non-Web Administrator 31
Installing Historian Data Collectors 31
Steps to Install Data Collectors 31
Installing the Historian Excel Add-In 32
Installing the Historian Client Tools 33
Installing the Historian HDA Server 34
Installing Historian SDK 35
Installing Historian Client Access API 35
Uninstalling Historian and Historian System Components 36
Upgrading from a Previous Release 36
Uninstalling the old Historian Product 37
Installing the new Historian Product 37
Upgrading the Historian SDK 38
Migration Tool 39
Using Migration Tool 39
Configuring Migration Options 40
Command-line Options for the IHA Migration Tool 43
Interoperability of Historian Versions 44
Troubleshooting 45

Implementing Historian Security 48
Protecting Your Process 49
Implementing Strict Authentication 49
Disabling Strict Client or Collector Authentication 51
Troubleshooting Strict Authentication Issues 51
Creating and Implementing a Security Strategy 52
Historian Login Security 53
Historian Security Groups 53
Historian Group Rights 54
Security Setup Example 59
Setting up Historian Security Groups 61
Setting Local Groups on Windows Systems 61
Avoiding Unauthorized Access When Using Historian Security 63
Working with Domain Security 63
Creating Security Groups in Windows 2003 Domain Controller 64
Creating Security Groups in Windows 2008 Domain Controller 64
Using a Windows 2003 Domain Controller with a Windows 2008 Historian Server 65
Configuring DataArchiver to use Active Directory Service Interface 66
Establishing Your Security Rights 68
Identifying the Security Checking Process 68
Implementing Tag Level Security 70
Retrieving Data from Historian 70

Sampling Modes 71
Calculation Modes 74
Query Modifiers 77
Filtered Data Queries 81
Overview of Filtered Data Query Parameters 82
Example: Filtered Queries in the Excel Add-In 85
Using Historian with iFIX 87
Using iFIX drivers with Historian 88
Collecting iFIX Alarm and Event Data 88
Viewing Historian Values and Time Stamps in an iFIX Chart 89
Importing the Historian Toolbar into iFIX 89
Using the Toolbar Buttons 89
Formatting OPC Tags Containing Special Characters 89
Filtering Tags Using THISNODE with Expression Builder 90
The iFIX Data Collector 90
Historian and iFIX Chart Objects 91
Browsing iFIX Tags On Networked iFIX Nodes 91
Creating Historian Charts using Mixed Pens 91
Using the iFIX Expression Editor to search tags 91
Searching for Calculation or Server-to-Server tags in the iFIX Expression Editor 92
Using the iFIX Integration Toolkit 92
Uninstalling Historian if iFIX v2.6 is installed 92

Using v7.x Drivers with Historian 93
Using Autocreate 93
Using the Latched Data feature 93
Running iFIX 7.x Drivers as OPC Servers 93
Running iFIX 7.x Drivers as a service with Automatic Startup 93
Troubleshooting iFIX and Historian 96
Running iFIX as a service with Workspace listed in the SCU Task List 96
iFIX Workspace delay when remote session is lost 96
Starting iFIX when a remote Historian session is unavailable 96
Accessing Mission Control when a remote Historian session is lost 97
Using the iFIX V2.6 chart with Historian domain security enabled 97
Accessing tags in the iFIX chart after setting OPC Collector to "Made After Restart" 97
Collecting data in an iFIX chart with Time Assigned By Source 97
Synchronizing the time on iFIX SCADA Servers and View Clients 97
Startup Procedure Overview 98
Contact GE Intelligent Platforms 99
General Contact Information 99
Technical Support 99

Getting Started with Historian

Before you begin installing Historian, please take some time to review the Getting Started with Historian manual.

This manual includes information about the following:

- An Overview of Historian
- Setting up the Historian Environment
- Installing Historian
- Implementing Historian Security
- Retrieving Data from Historian
- Using Historian with iFIX

This manual provides descriptive material and specific operating procedures for performing all common tasks.

Reference Documents

For related information about Historian, refer to the following documents:

- Using the Historian Administrator
- Historian Data Collectors
- Using the Historian Excel Add-In
- Historian Alarms and Events
- Migrating Advanced and Classic Historian Data
- Using the Historian OLE DB Provider
- Historian Software Development Kit (SDK) Online Help System

What's New in Historian 5.5

Multi Field User Defined Data Types

Proficy Historian now gives you the ability to create a new user defined data type which includes multiple fields of any data type and then create Historian tags of that type. All the regular tag operations can be performed on this tag. You can perform raw and calculated queries on the collected data.

For more information, refer to the User Defined Type topic in the Using the Historian Administrator e-book in the online help.

Dynamically Sized Array Tags

Proficy Historian now allows you to store a set of values with a single timestamp and then read the elements back individually or as an array tag.

For more information, refer to the Array tag topic in the Using the Historian Administrator e-book in the online help.

Enhanced Data Query Filtering

With Filter Expression you can now enter complex filter conditions that instruct the Data Archiver to examine the collected data and return time ranges that match the condition so that those ranges can be queried further.

For more information, refer to the Using Filter Expression topic in the Advanced Topics e-book in the online help.

Updated Operating System Support

Proficy Historian 5.5 supports running on Windows 8 and Windows Server 2012.

Permanent Rename and Permanent Delete of Tags

You can now efficiently manage your tags and memory by truly deleting or renaming tags to meet your current

needs instead of aliasing them and hiding the tags. Truly renaming or deleting the tags that are no longer needed saves disk space and memory and makes the names available for re-use.

For more information, refer to the Permanently Rename a Tag and Permanent Delete a Tag topics in the Using the Historian Administrator e-book.

New Calculation Modes

Proficy Historian now has the following additional calculation modes that add more combinations and contexts for data retrieval:

- **FirstRawValue/FirstRawTime** retrieves the first good raw sample value or timestamp for a given time interval.
- **LastRawValue/LastRawTime** retrieves the last good raw sample value or timestamp for a given time interval.
- **Tagstats** returns multiple calculation modes for a tag in a single query.

For more information, refer to the Calculation Modes topic in the Advanced Topics e-book.

New Query Modifiers

Proficy Historian now provides new Query Modifiers that alter the behavior of Sampling and Calculation Modes to meet your retrieval requirements.

- **INCLUDEBAD** directs the Data Archiver to consider raw samples of bad data quality when computing calculation modes. You can use this modifier to consider both good and bad quality values.
- **FILTERINCLUDEBAD** the FILTERINCLUDEBAD modifier directs the Data Archiver to consider the values of bad quality data when determining the time ranges that match the filter condition.
- **USEMASTERFIELDTIME** returns raw values of all the field elements in a multifield type tag at the timestamp determined by the MasterField.

For more information, refer to the Query Modifiers topic in the Advanced Topics e-book.

New Comparison Modes

Proficy Historian now allows you to do a bitwise comparison for a tag. By using bitwise comparison you can compare the binary values of the given filter tag with the bits specified in the condition. The Bitwise

comparison modes are:

- **AllBitSet (^)** comparison mode returns True when the binary value of the Filter Tag is equal to all the bits in the condition.
- **AnyBitSet (~)** comparison mode returns True when the binary value of the Filter Tag is equal to any of the bits in the condition.
- **AnyBitNotSet (!~)** comparison mode returns True when the binary value of the Filter Tag is not equal to any one of the bits in the condition.
- **AllBitNotSet (!^)** comparison mode returns True when the binary value of the Filter Tag is not equal to all the bits in the condition.

For more information, refer to the Using Filter Expression topic in the Advanced Topics e-book.

New Sampling Mode

Proficy Historian now gives you a new sampling mode which can be used on retrieval of data that has already been collected in the arhive.

RawByFilterToggle sampling mode is a form of filtered data query. A filtered data query returns data values for a particular time period whereas RawByFilterToggle sampling mode returns the time periods where the condition becomes TRUE or FALSE.

For more information, refer to the Sampling Modes topic in the Advanced Topics e-book.

Overview of Historian

Proficy Historian is a high performance data archiving system designed to collect, store, and retrieve time-based information at extremely high speed efficiently. The system architecture consists of the following:

Historian Server: The Historian server is the central point for managing all of the client and collector interfaces, storing and (optionally) compressing data and retrieving data. All tag data (numbers, strings, BLOBs) are stored in a proprietary format in the archive database. The Archive Database consists of several files, each of which represents a specific time period of historical data.

If licensed for the ”Alarm and Event” option then the server also manages the storage and retrieval of OPC alarms and events in a SQL Server SQL Server Express.

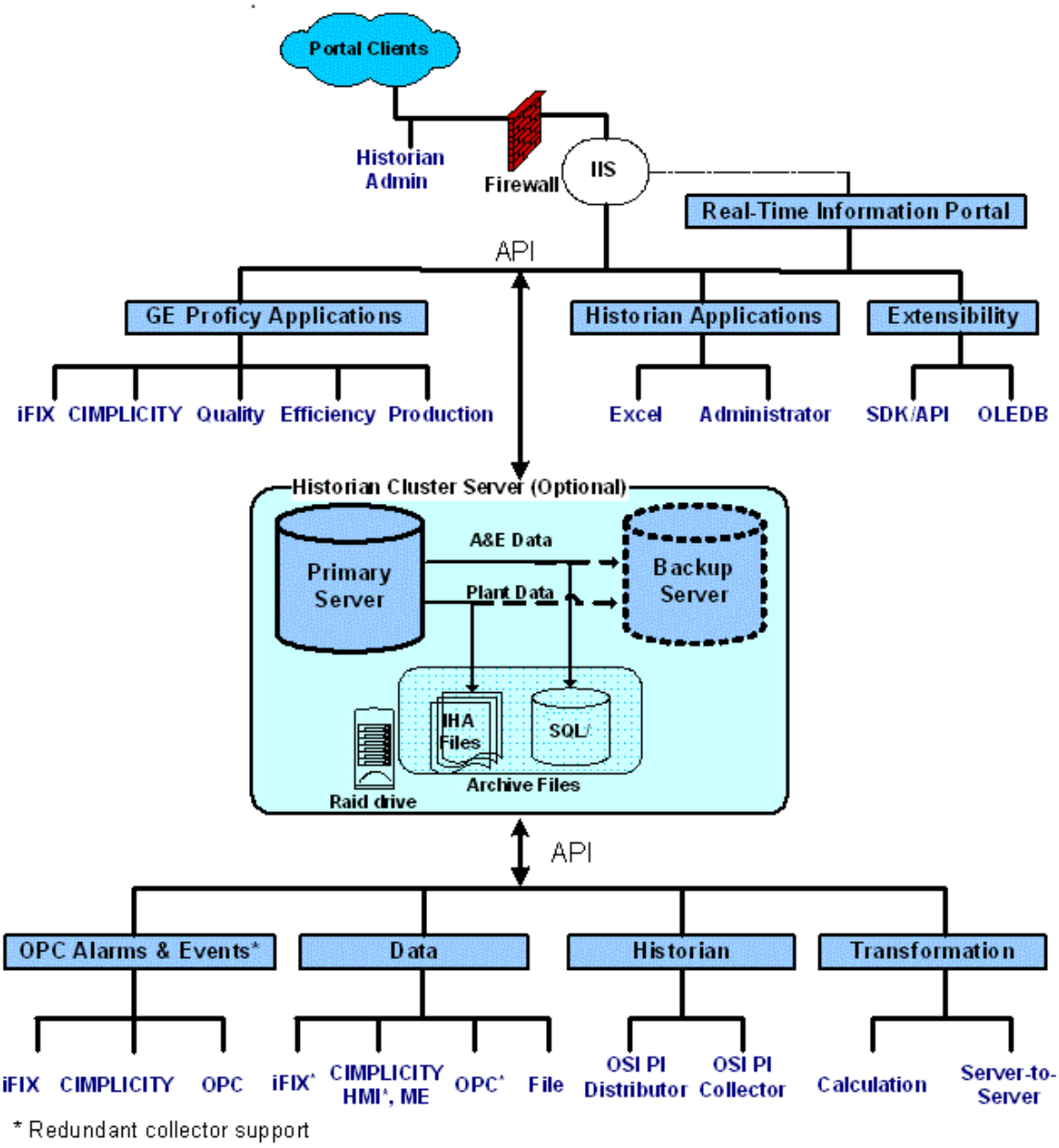
Collectors: The Historian includes several types of data collectors for collecting data from a wide variety of applications including: iFIX, Proficy Machine Edition, OPC, OPC Alarms & Events, Text Files (csv or xml), and OSI PI.

> ***NOTE:*** *To collect data from a CIMPLICITY, you must use the Historian OPC collector with the CIMPLICITY OPC Server*

The Calculation collector is designed to perform math and analysis on Historian data and store the results in tags, on the server. The Server-to-Server collector has the same calculation capabilities as the Calculation collector, but it stores the results in tags, on a remote server.

Most collectors are capable of performing first-order ”dead band” compression as well as a ”browse & add” configuration and store & forward buffering.

Clients: All client applications retrieve archived data through the Historian API. The Historian API is a client/server programming interface that maintains connectivity to the Historian Server and provides functions for data storage and retrieval in a distributed network environment.



Typical Historian System

The Historian Archive indexes all information by Tagname and Timestamp. The Tagname is, a unique identifier for a specific measurement attribute. For iFIX users, an Historian Tagname normally represents a Node.Tag.Field (NTF). Searching by Tagname and Time Range is a common and convenient way to retrieve data from Historian. If you use this technique to retrieve data from the Archiver, you do not need to know which archive file on the Historian Server contains the data. You can also retrieve data using a filter tag.

Historian is capable of storing many different data types, such as Floating Point, Integer, String, and BLOB (undetermined binary data type), such as an Excel spreadsheet, a PDF file, or a Word file. The source of the data defines the ability of Historian to collect specific data types.

System Components

A Typical Historian System contains several components:

- One or more Historian Data or alarm Collectors to data sources
- One or more Historian Servers for data or alarms
- One or more Historian Non-Web Administrators
- Historian OLE DB provider
- One or more Historian HDA Servers
- One or more Excel Add-In packages, installed on any client node
- Programs using Historian User API
- Programs using Software Development Kit (SDK)

All clients communicate with the Server through the Historian API. The subsections that follow list the functions performed by each component.

Historian Alarms and Events

Historian Alarms and Events provides tools to collect, archive, and retrieve alarm and event data in Historian.

Refer to the Historian Alarms and Events manual for more information

Historian Data Collectors

Data Collectors are the interface between a data source and the data archiver. They:

- Collect data using a specific acquisition interface, such as iFIX EDA, OPC Alarms and Events,

Machine Edition View, OSI PI, or OPC 1.0 or 2.0.

- Perform first level data compression (deadband/update by exception).
- Buffer data (store and forward) whenever a server connection is lost.

Refer to the Historian Data Collectors manual for more information.

Historian File Collector

File Collectors import .CSV or .XML files into Historian. The files can contain data, alarms, tagnames or other configuration information, and messages that you can import with a File Collector.

Refer to the Historian Data Collectors manual for more information.

Historian Administrator

An Historian Administrator provides a graphical user interface for performing Historian maintenance functions including:

- Tag addition, deletion, and configuration.
- Maintaining and backing up archive files.
- Data collector configuration.
- Security configuration.
- Searching and analyzing system alerts and messages.

Refer to the Using the Historian Administrator manual for more information.

Historian Server

An Historian Server performs the following tasks:

- Manages all system configuration information.
- Manages system security, audit trails, and messaging.
- Services write and read requests from distributed clients.
- Performs final data compression.
- Manages archive files.

Excel Add-In

The Historian Excel Add-In is a very useful tool for presenting and analyzing data stored in archive files. Using this tool, you can design custom reports of selected data, automatically process the information, and analyze the results. You can also use it for performing tag maintenance functions in Historian, such as adding tags, importing or exporting tags, or editing tag parameters.

Refer to the Using the Historian Excel Add-In manual for more information.

Historian OPC HDA Server

The Proficy Historian OPC HDA Server reads the raw data stored in Historian and sends it to the connected OPC HDA clients. The Proficy Historian OPC HDA Server is in compliance with OPC Server HDA 1.20 standards.

Refer to the Historian OPC HDA Server manual for more information.

Historian User API

The Historian User API is intended to provide high speed read/write access to Historian data and read access to Historian tags. There is no access to alarms, events, or messages.

Use the API to develop applications in C or C++, which read and write data to the Historian server when the Historian SDK and Historian OLEDB do not meet your project requirements for performance or programming language.

Proficy Historian allows you to develop both 32-bit and 64-bit User API programs.

NOTE: *If you want to build a 32-bit User API program on a 64-bit operating system, then you need to rename the ihuapi32.lib to ihuapi.lib and include it in your program.*

Refer to the ihUserApi Help system for more information.

Historian SDK

The Software Development Kit (SDK) is designed for writing Visual Basic (VB) or Visual Basic for Applications (VBA) Scripts. Using the SDK, you can develop your own scripts to perform selected repetitive or complex tasks or to make your own custom user interface. To use the SDK, create a VB/VBA project with the SDK as a project reference.

Refer to the SDK Help system for more information.

Historian Client Access API

Most applications today rely on .Net based development platforms from Microsoft. To enable easier integration with Historian, a .Net API is provided. The Client Access API supports both 32-bit and 64-bit Windows Operating Systems.

Historian Migration Tools

Historian provides migration tools to allow you to migrate your existing Classic Historian configurations and data and your iFIX Alarm and Event data into the Historian environment. Tags, collection rates, and deadbands for tags configured in Classic Historian can be transferred into Historian by the migration tools.

Refer to the Migrating Advanced and Classic Historian Data manual for more information.

Understanding the System Architecture

You have wide flexibility in configuring your Historian application. Since Historian can support a fully distributed architecture, you can spread the data collection, server, administration, and client data retrieval functions across many different nodes in a network, or you can install all components on a single computer.

Since the Historian API is the basic building block for connectivity, all Historian functions, including data collection, administration, and data retrieval, use the Historian API.

You can connect the Historian API to a local Historian Server in the same manner as to a remote Historian Server by simply providing the name of the server. This name must be the Computer Name or IP Address of the target Historian Server, and the server must have TCP/IP connectivity. If you use the Computer Name of the server rather than the IP Address, the IP Address must be available to the client through DNS, a WINS server, or through the local host table.

It is recommended that you install the Historian Server on a central dedicated server, as shown in the Typical Historian System figure. Next, install data collectors on each data source, and point them back to the central Historian Server by specifying the appropriate server Computer Name. Install a separate data collector for each type of collection interface used in your system.

Observe the following constraints when you install collectors:

iFIX Collector, File Collector, Simulation Collector, Calculation Collector, Server-to-Server Collector, Windows Performance Collector, or – install only one collector of each type per computer.

OPC Collectors – install only on a computer where the OPC Server is running locally. You can install multiple collectors on a single computer, however, by installing a collector for each OPC Server.

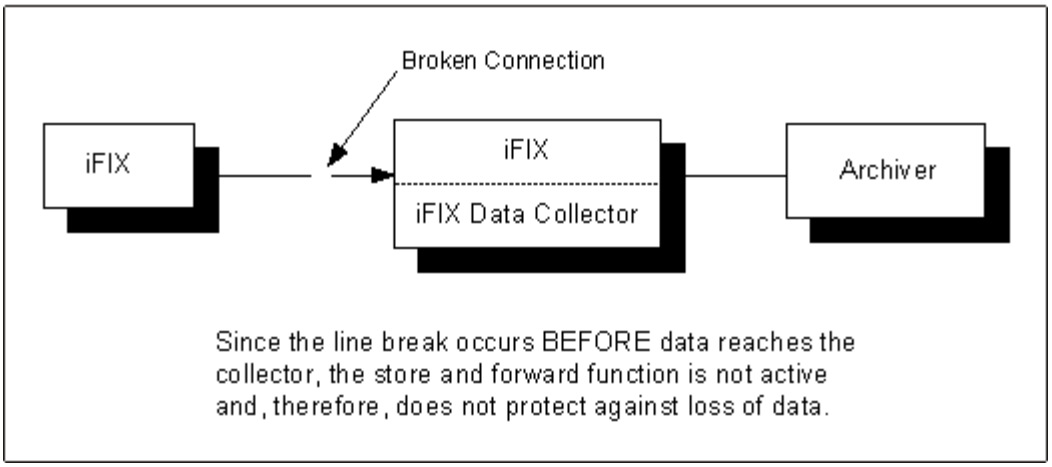
You can install various types of collectors on a single computer, subject to the preceding constraints.

iFIX Implementation Guidelines

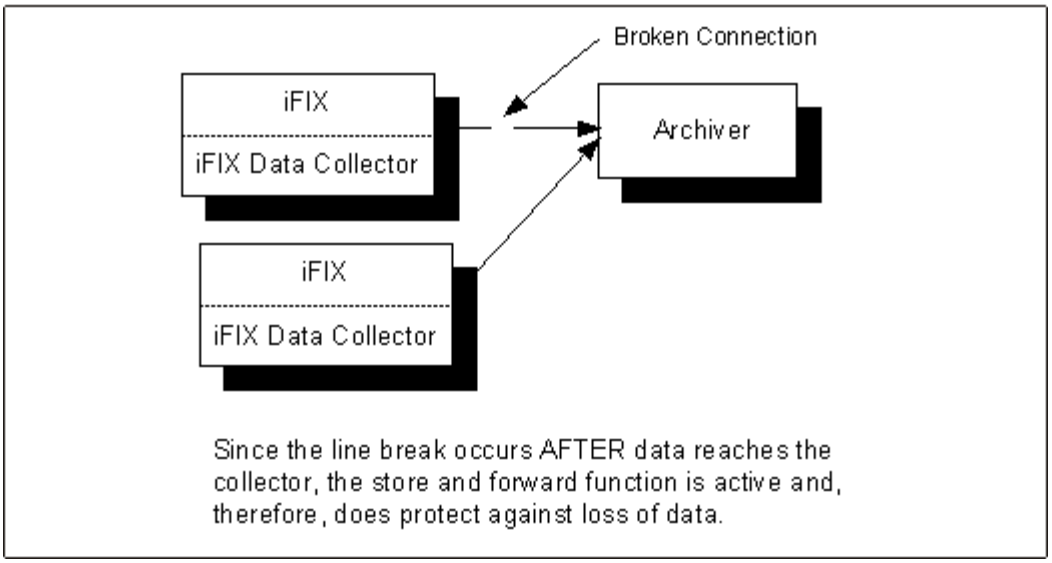
With an iFIX implementation, install data collectors on each SCADA Server that contains the Node.Tag.Fields (NTFs) you want to collect. You can minimize system load in this way because you are not relying on FIX networking to pull remote data into the node where the collector is running.

In a distributed environment, remote data collectors automatically buffer collected data in the event of loss of a network connection between the collector and the Historian Server. When the network connection is re-established, the data collectors automatically re-establish data flow and forward all buffered data to the server.

The store and forward feature does not apply when you use iFIX networking for data collection. Since iFIX network connections are located ahead of the data collector in the data flow path, the store and forward feature does not protect against loss of data when an iFIX network connection is interrupted, as illustrated in the following figure.


Broken Connection
iFIX
iFIX
iFIX Data Collector
Archiver
Since the line break occurs BEFORE data reaches the collector, the store and forward function is not active and, therefore, does not protect against loss of data.

Ineffective Use of Store and Forward in an iFIX Network


Broken Connection
iFIX
iFIX Data Collector
Archiver
iFIX
iFIX Data Collector
Since the line break occurs AFTER data reaches the collector, the store and forward function is active and, therefore, does protect against loss of data.

Effective Use of Store and Forward in an iFIX Network

Historian Alarm and Event Archiving

Historian's Alarm and Event (A&E) archiving offers the ability to collect A&E data from any OPC-compliant A&E server and store it in an integrated relational database (SQL Server Express). Historian Alarm and Event data is associated with the related process data from its source to allow for quick analysis.

For more information, refer to Historian Alarms and Events.

Setting up the Historian Environment

Before you start setting up your Historian environment, identify the computers that will function as your clients, data collectors, administration workstations, and archiver. The following sections outline the setup procedures in detail.

Task Overview

When you are ready to set up your Historian environment, use the following procedure:

1. Set up each computer.

   Use the section Hardware Requirements as a guide, and refer to the user manual that accompanies each computer for detailed setup information.

2. Use a login account with administrator rights so that you can install Historian later.

   NOTES:

   - *Historian installer will automatically detect and install 32-bit or 64-bit Historian 5.5 Server based on a system architecture.*

Use the section Software Requirements as a guide, and refer to the user manual that accompanies each software product for more detailed setup information.

3. Install the Hardware Key on your Historian Server node only.

   Refer to the section Installing the Hardware Key for instructions on attaching the key to your computer.

4. Disable the Guest account in Windows security if you want to limit authentication to known Windows users only.

Hardware Requirements

For Historian Servers, the minimum hardware requirements are:

- A 2.4 GHz clock speed Intel Core i3 or i5 or i7 CPU or equivalent AMD Phenom CPU with 4 GB RAM for a 32-bit Historian Server and 4 GB RAM for a 64-bit Historian Server.
- A DVD-ROM drive.
- 100 Mbps TCP/IP-compatible network interface adapter for network communication and certain I/O drivers.
- 80 GB free hard drive space for the data archives, message files, buffer files, and log files used by the system.

For Data Collector nodes, the recommended minimum hardware requirements are:

- A 2.0 GHz clock speed Intel Core i3 or i5 or i7 CPU or equivalent AMD Phenom CPU with 2 GB RAM.
- 40 GB of free hard drive space to store buffered data.
- A DVD-ROM drive.
- TCP/IP-compatible network interface adapter for network communication and certain I/O drivers.

For the Microsoft Cluster service, the minimum hardware requirements are:

- A 2.6 GHz clock speed Intel Core i3 or i5 or i7 or Xeon or equivalent AMD Opteron CPU with minimum 8 GB RAM.
- Two 100Mbit TCP/IP-compatible network interface adapters for network communication and certain I/O drivers (one for public network, another for private network).
- 40 GB shared SCSI hard drive (RAID preferred).
- 80 GB of local free hard drive space.

NOTE: *The configuration of each server added to the cluster must be identical to the other servers in the cluster.*

You determine the size of an Historian Server as a function of the number of tags from which data is collected, the rate of alarm and event collection, and how often you intend to collect the data and how much data you want to keep online. The number of tags is an indicator of the number of concurrent users likely to access the system. The primary factor is server memory requirements; CPU load is a secondary factor. If the number of concurrent users is significantly different from the suggested guidelines, adjust server memory size accordingly.

Use the following parameters to determine the size of the Historian Server.

Recommended Historian Server Configurations*						
Tags	<10K	10K to 100K	100K to 1 Million	1 Million to 2 Million	2 Million to 10 Million	10 Million to 20 Million
RAM (GB)	4 GB	4 GB	32GB	64 GB	128GB	256GB

Disk Size required	80 GB	160 GB	1 TB	4 TB	10TB	15TB
Processor Type	Intel Core-i5, i7 family, or equivalent		Intel Xeon (56xx, E5 family or AMD Opteron 42xx/62xx family)		Intel Xeon (56xx, E5 family or AMD Opteron 42xx/62xx family)	Intel Xeon (56xx, E5 family or AMD Opteron 42xx/62xx family)
CPU	Dual/Quad cores		2-Socket		2-socket or 4-socket	2-socket or 4-socket
CPU Speed (GHz)	2.8		2.6		2.6	2.6
Recommended CPU clock in Giga Hz	2.8		2.6		2.6	2.
Operating System	Windows 7 (32-bit) or Windows Server 2008 (32-bit)		Windows Server 2008 R2/Windows 2012 standard (64-bit)		Windows Server 2008 R2/Windows 2012 standard (64-bit)	Windows Server 2008 R2/Windows 2012 standard (64-bit)

Storage Type	Internal SATA Drives	Direct attached or shared storage with SAS enterprise class drives. Hardware RAID controller with cache memory	High speed shared storage with SAS or SSD drive types. Hardware RAID controller with cache memory	High speed shared storage with SAS or SSD drive types.
Years of data online	1 year			

*Above recommended configurations may vary based on years of data online, update rate, data compression setting, and other tag configuration parameters.

***NOTES**:*

1. *Proficy Historian Server can run on both 32-bit and 64-bit versions of Windows.*
2. *Sustained event rate is 18 million per minute.**
3. *Proficy Historian supports Intel Core i3, i5, i7 Duo based processors as long as they are compatible with the operating system.*
4. *Proficy Historian does not support Itanium processors.*

Example System for Sustained Event Rate

Specification	**Medium Size Server**	**Large Size Server**
Processor Type	Intel Xeon 5540	Intel Xeon E5-2670 or E5-4650
CPU	Dual socket	Dual socket or quad-socket

CPU Speed (GHz)	2.5	2.7
RAM (GB)	64	256

***NOTE**: The system performance may vary depending on the hardware specifications, operating system, and tuning parameters. The above hardware specifications are provided as a reference only.**

Recommended Historian Collector Configurations:

Recommended Historian Collector Configurations*	
RAM (GB)	2 GB*
Disk Size required	40 GB
Historian 5.5 Collectors	32-bit
Operating System	Windows 7 (32-bit) or Windows 7 (64-bit)**

*Historian 5.5 Collectors may use up to 4 GB RAM in a 64-bit Windows operating system.

**Historian 5.5 Collectors work as 32-bit applications on a 64-bit Windows operating systems using WoW64 mode (Windows-on-Windows 64-bit). However, you can read and write data from a 64-bit Historian Server.

NOTES:

1. *RAM and Disk Size required may vary based on the collectors available on the system.*
2. *Recommended number of tags per collector is 20 to 30K.*

For iFIX systems, count each Node.Tag.Field (NTF) as a separate tag when you determine the size of the system. For example, FIX.FIC101.F_CV and FIX.FIC101.B_CUALM (current alarm) both count as tags, even though they are derived from the same iFIX tag.

Use the following parameters to determine the size of the Historian Alarm and Event archiver.

Alarm & Event Rate	RAM	CPU
1 / minute	1 GB	Single
1 / second	2 GB	Single
10 / second	2 GB	Single
100 / second	4 GB	Double

You must have disk storage capacity in the multi-GB range for the many data archive files (typically 500 MB each) and alarms you will generate, especially if you want to keep old data online.

NOTE: *As more applications run simultaneously on a server, performance decreases. Whenever possible, run additional applications on separate computers.*

Hardware Requirements - Proficy Historian on Windows XP Embedded

The minimum Historian software requirements are:

- A minimum Atom-based 1.6 GHz computer or equivalent.
- A minimum of 1 GB RAM.
- A minimum of 1 GB of free hard drive space (for an upgrade). For a new installation, a minimum of 5 GB of free hard drive space is required.
- Other GE Intelligent products, such as Proficy iFIX, impose additional requirements. Refer to the Important Product Information (IPI) topic in the product's electronic books for specific system requirements. Click the System Req. tab in that product's IPI for details.
- TCP/IP-compatible network interface adapter for network communication and certain I/O drivers. One free, direct-connect USB port. Some touch screens, pointing devices, and I/O drivers require a serial port. Additional ports for I/O hardware should be ordered with the computer.
- SVGA or better color graphics monitor and a 100% IBM-compatible, 24-bit graphics card capable of 800x600 resolution and at least 16 million (16,777,216) colors.
- Two-button mouse or compatible pointing device (such as a touch screen).

  NOTE: *There are risks associated with using a Compact Flash or a similar device as a Primary drive in the Windows XP Embedded environment with the Proficy Historian product and your production data.*

These types of devices have a lifetime associated with them regarding the number of writes the device is capable of over a lifetime. As such, storing production data on such a device may result in lost data, over the long term. If the system has a physical drive, and not a Compact Flash or a similar device, the production data is affected by this risk.

Recommended Historian Server Configurations* on Windows XP Embedded	
Tags	<100K
RAM (GB)	2 GB
Disk Size required	80 GB
Historian 5.5 Server	32-bit
Processor Type	Xeon, or Intel Core-i5, i7 family, or equivalent
CPU	Dual/Quad cores
CPU Speed (Ghz)	2.8
Storage Type	Internal SATA Drives
Years of data online	1 year

*Above recommended configurations may vary based on years of data online, update rate, data compression setting and other tag configuration parameters.

Software Requirements

The minimum Historian software requirements are:

- One of the following operating systems, with latest service packs or revisions:
    - Windows XP Professional SP3 (32-bit or 64-bit)

- Windows XP Embedded (32-bit)
- Microsoft® Windows® 7 Professional (32-bit or 64-bit)
- Microsoft® Windows® 8 Professional (32-bit or 64-bit)
- Microsoft® Windows® Vista Professional (32-bit or 64-bit)
- Microsoft® Windows® Server 2003 (32-bit or 64-bit)
- Microsoft® Windows® Server 2003 R2
- Microsoft® Windows® Server 2008 R2 (64-bit)
- Microsoft® Windows® Server 2008 R2
- Microsoft® Windows® Server 2012 Standard (64-bit)

NOTES:

- *Historian 5.5 32-bit components such as Collectors, Excel Add-in 32-bit, Interactive SQL 32-bit, APIs, and Non-Web Administrator, work as 32-bit application on 64-bit Windows operating systems using WoW64 mode (Windows-on-Windows 64-bit). However, you can read and write data from a 64-bit Historian Server.*
- *If you are going to use Proficy Historian 5.5 on Windows Server 2008 (32-bit or 64-bit) or Windows Server 2008 R2 you must go for a Full Installation not Core Installation of Windows.*
- *SQL must use mixed mode authentication.*
- *The collation for your Alarm and Event database needs to match the collation of your SQL Server. This happens automatically by default but can become different if the Alarm and Event Database is moved to another SQL Server.*

- Network interface software for network communication. The TCP/IP network protocol is required.
- One of the following 32-bit or 64-bit SQL Server systems to configure alarm and event archiving:
  - Microsoft SQL Server 2008 Standard, Professional, R2 or Enterprise Edition
  - Microsoft SQL Server 2008 Express
- One of the following 32-bit or 64-bit versions of SQL Server to use Historian as a linked server:
  - Microsoft SQL Server 2008 Standard, Professional, or Enterprise Edition
  - Microsoft SQL Server 2005 Standard SP2, Professional SP2, or Enterprise Edition SP2
  - Microsoft SQL Server 2008 Express
- The Historian Excel Add-In requires installation of Microsoft Office 2003, or Microsoft Office 2007, or Microsoft Office 2010 (32-bit/64-bit).

Compatibility with other Proficy Products

Several GE Intelligent Platform products work with Proficy Historian. The following is a general set of required versions to work with Historian 5.5 on the same computer.

***IMPORTANT**: If you want to enable the new Strict Authentication feature in Proficy Historian 5.5, be aware that you will need to apply the latest SIMs that support this feature for all Proficy clients that connect to the Archiver, including the ones listed in this table. In addition, there may be SIMS to allow pre-5.0 collectors and client applications such as Excel Add-In to connect. Refer to the SIM download page for update for Historian and other Proficy products.*

Product	Required Version
Proficy Portal	3.5, 3.5 SPI1.
Machine Edition View	7.5, 7.0
CIMPLICITY	8.2, 8.1, 8.0.
iFIX	5.5, 5.1. *
Plant Apps	6.1, 5.0, 4.1.**
Proficy Workflow	2.1, 2.0.

Proficy Smart Signal	5.5
Proficy CSense	5.5
PHA	5.5, 5.0

* For customers using iFIX, there was a change in the HKEY_CURRENT_USER registry values for WebSpace and it will no longer work with the existing sim. Ensure that you get the latest iFIX sims. The following article provides additional instructions:

http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15129

* For customers using iFIX 5.1 and 5.0 with Historian 5.5, there is a change in the registry entry that has to be updated. The following article provides additional instructions:

http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB13651

** For Plant Apps customers using the Historian Type = GE Proficy - Historian 3.0 to connect to Proficy Historian 5.5, both the Enabled and Disabled options for Enforce Strict Client Authentication selection are supported.

** For Plant Apps customers using the Historian Type = GE Proficy - Historian to connect to Proficy Historian 5.5, only the Disabled option for Enforce Strict Client Authentication selection is supported.

In Historian 5.0, the Historian HKEY_CURRENT_USER registry key values were changed. The programs accessing the server collection through the SDK are unaffected. Any program or script that directly accesses the registry keys or any Terminal Server login scripts that try to configure a list of servers by importing registry keys directly will no longer work. Such programs need to access the server collection via SDK calls, not directly.

Supported Regional Settings

Historian supports the following regional settings available in the Windows Control Panel:

- Decimal symbol - one character
- Digit grouping symbol

- List separator - one character
- Time style
- Time separator
- Short date style
- Date separator

Time and Date Formatting

Avoid changing the time style or short date style in regional settings to values that are outside of the standard styles provided. Changing these values to non-standard styles may result in improperly formatted times and dates.

Historian supports the following short date formats, some of which may not be available in certain language versions of Windows:

- dd/mm/yy
- dd/yy/mm
- mm/dd/yy
- mm/yy/dd
- yy/dd/mm
- yy/mm/dd

Supported Data Types

The following table lists the supported Historian data types and their sizes:

Data Type	**Size**
Single Float	4 bytes
Double Float	8 bytes

Single Integer	2 bytes
Double Integer	4 bytes
Quad Integer	8 bytes
Unsigned Quad Integer	8 bytes
Unsigned Single Integer	2 bytes
Unsigned Double Integer	4 bytes
Byte	1 byte
Boolean	1 byte
Fixed String	Configured by user.
Variable String	No fixed size.
Binary Object	No fixed size. Historian does not support the use of the Binary Object data type with the Data Collectors. Refer to the SDK online Help for more information on working with BLOB data types.
Scaled	2 bytes

The Hardware Key

You are required to use a hardware key to run Historian Server. The hardware key:

- Enables software options available to your installation, as requested by you.
- Can be electronically reprogrammed using an upgrade utility, as requested by you. Consequently, you are no longer required to exchange hardware keys for version updates or option changes.
- Protects against illegal duplication of Historian software.

Additionally, two hardware keys are offered: one that supports parallel port configurations, and one that supports USB port configurations.

Historian runs in demo mode (one user, 100 tags) if the key is not installed.

NOTE: *File the packing slip that came with the hardware key in a safe place. The codes on this slip are necessary to quickly duplicate the key in case it is damaged or misplaced.*

Installing the Hardware Key

To install the hardware key:

1. Power off the computer and all peripheral devices prior to installing the hardware key; it is sensitive to static electricity.
2. Remove any connections to your computer's parallel port.
3. Secure the hardware key in the parallel port and tighten the screws.

   IMPORTANT: *Do not remove the hardware key from your node while Historian Server is running. If you do remove the key while running, the server will shut down when the next key check is performed, which occurs every two hours. When no key is attached, Historian defaults to demo mode. When you exceed the demo mode defaults of one user connection and 100 tags, the Historian Data Archiver stops; this is intended licensing behavior.*

4. If you had any equipment connected to your parallel port, connect it to the back of the hardware key. If you are using a USB port for the hardware key, you cannot plug any other equipment into the port. Use another port for any additional equipment connections you may need.

The number of tags and clients that you are licensed to use appears in the System Statistics screen of the Historian Administrator. If the Licensed Tags field displays 100 tags and the Licensed Users field displays 1 client, ensure that you have correctly installed your hardware key.

Disabling Guest Accounts

Whether or not you use Historian security, make sure that you disable Guest accounts on your computer. It is recommended that you disable Guest accounts so that Historian operates in the most secure environment,

limiting the users to known Windows users.

Optimizing Virtual Memory

Through the use of paging files, Windows allocates space on your hard drive for use as if it were actually memory. This space is known as virtual memory. Be sure to optimize the virtual memory on the Historian archiver computer. The following list describes how to optimize virtual memory in Windows to achieve maximum performance from Historian.

To optimize the virtual memory paging file for Historian in Windows:

1. Double-click the System icon in the Windows Control Panel.
2. Open the Performance Options:
    - On Windows XP or Server 2003; click the Advanced tab, under Performance, click Settings. In the Performance Options dialog box, click the Advanced Tab.
    - On Windows Vista, Windows 7, or Windows Server 2008; click Advanced System Settings In the left pane. On the Advanced tab, under Performance, click Settings. In the Performance Options dialog box, click the Advanced Tab.
3. In the Virtual Memory group box, select Change.
4. In the Initial Size field, enter a value equal to three times your physical memory.
5. In the Maximum Size field, enter a value equal to three times your physical memory.
6. Select Set.
7. Click OK to save the changes and exit the dialog box.

NOTE: *If the paging file is set to grow dynamically, your system may experience severe performance problems during run time. To ensure optimal performance, be sure that the Initial Size and Maximum Size of the paging file are the same so that the paging file does not grow dynamically. For more information on creation and sizing of Windows paging files, refer to the Microsoft Windows Help.*

Using a Remote SQL Server to Store Alarms

If you have chosen to connect Historian to a remote SQL Server, you must ensure the following conditions are met:

- The Historian Alarm Archiver service must be run on a user account that has privileges to log into the SQL Server using Windows Authentication.

- The Default Backup Path, found on the Archive screen, must be a shared directory that is accessible to both the Historian Data Archiver and the remote SQL Server. It is recommended that this shared directory be placed on the same computer as the Historian Data Archiver service.

Installing Historian Software

Proficy Historian provides a single install program on a DVD with options that install each system component. Before running the installation program, define the desired system architecture and determine which components you want to install on each node.

You can now install **Proficy Historian 5. Server** on both 32-bit (x86) systems and 64-bit (x64) systems. Historian 5.5 installer automatically detects and installs a 32-bit or 64-bit Historian 5.5 Server based on system architecture. All the other Historian 5.5 components such as Collectors, Excel Add-in 32-bit, SQL Linked Server 32-bit, APIs, and Non-Web Administrator work as a 32-bit application on 64-bit Windows operating systems using WoW64 mode (Windows-on-Windows 64-bit). However, you can read and write data from a 64-bit Historian Server.

Installing Proficy Historian 64-bit server not only takes a full advantage of all the memory in your 64-bit Windows operating system but also boosts overall Proficy Historian performance, security, and admin responsiveness.

NOTE: *To install a data collector, you must first install the source software. If you have added new source software since installing Historian, you must re-run the Historian install. Keep currently installed components checked when reinstalling Historian. Some components may be restarted when installing new data collectors.*

If you are installing all system components on a single computer, run the single step installer (Historian Installer) on that computer only. If you plan to use multiple computers as server, data collector, administrator, and other clients, run the respective installer (Historian Server, Historian Collectors, or Historian Client tools) on each computer to install the specific components needed for that computer.

If you are installing system components on a machine with any previous Historian components installed, the Install program automatically detects the already installed components and displays those items as checked in the components screen. Select the new components in addition to the already installed components, and continue through the upgrade.

Installing the Historian Server

You can now install **Proficy Historian 5.5 Server** on both 32-bit (x86) systems and 64-bit (x64) systems. Historian 5.5 installer automatically detects and installs a 32-bit or 64-bit Historian 5.5 Server based on system

architecture.

***NOTE:** If you intend to run all components (Historian Server, Collectors, and Client tools) on a single computer, click **Historian Installer** on the splash screen and proceed with the installation wizard.*

***NOTE:** If you choose to install the Alarm and Event Archiver then you must restart your computer to complete the SQL Server Express 2008 and Plant Database installations.*

To install the Historian Server:

1. Login to Windows with Administrator privileges. Ensure that there are no Proficy Historian or GE Intelligent Platforms' processes running, and close any other programs that are running.
2. At the computer you select as the server, insert the Historian DVD. The Historian splash screen appears.

   ***NOTE:** If this screen does not automatically appear, double-click the InstallFrontEnd.exe file on the DVD to display it. A message may appear with a security warning; click Run to proceed.*

   IMPORTANT:

   - *When you are installing Proficy Historian on Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008 or Windows Server 2008 R2, you must run the installer as an administrator. To run the installer as an administrator, right-click the InstallFrontEnd.exe and click "**Run-as administrator**".*

3. Click the "**Historian Installer**" link. A message box appears asking you to confirm the install.
4. Click Run to proceed. The install program starts and the Welcome screen appears.
5. Click Next to proceed. The License Agreement screen appears.
6. Click Yes to continue. The Select Features screen appears.
7. Select the components that you want to install, and then click Next. The Windows Firewall screen appears.
8. Select Yes, and then click Next. The Historian Server Security screen appears.
9. Select the user account that will be granted administrative access to Historian. The following options are available:
   - All Users - All local and domain account users will have full access to the Historian server. To control access, security groups may be configured post install, if required. By default, the All Users option is selected.
   - Specific User - Local or domain account user defined during installation will have full access to the Historian server as the selected user will be added to the iHSecurity Admins security

group. Other users can be granted restricted or administrator access post install.

a. To provide access to a specific user, enter the user name. Alternatively, click the **Browse** button. The Select User dialog box appears.

NOTES: *While entering a user name:*

- *The user name can be a local or domain account name.*
- *Ensure that only the user name is entered without adding the name of the computer or domain as a prefix.*

b. Enter the user name in the Enter the object name to select field and click Next.

- If you do not provide a valid user name, an error message appears indicating that it is not a valid user name.

10. Click Next. The Historian Collectors Configuration screen appears.
11. In the **User Name** and **Password** fields, enter the user name and password under which you want to run the collector services and then click Next.

- If you do not provide a user name and password, collector services will run under the local system account.

12. If you choose to install the Alarm and Event Archiver then you must specify the SQL Server details, and then click Next. The Choose the Program Folder screen appears. Refer to the Historian Alarm and Event SQL Configuration for more information on how to proceed.
13. Accept the default destination folder or browse for a new location, and then click Next. The Choose the Data (Archives) and Configuration folder screen appears.

NOTES: *On a 64-bit Windows Operating System:*

- *The default destination folder for a 64-bit Historian Server is* ***C:\Program Files\Proficy\Proficy Historian\x64\Server*** *directory.*
- *The default destination folder for all 32-bit components (such as collectors, client tools, and APIs) is* ***C:\Program Files\Proficy\Proficy Historian\x86*** *directory.*

14. Accept the default Historian Archives folder or browse for a new location, and then click Next. The Configuration Review screen appears.

NOTE: *Historian creates Log files and Buffer files folder inside Data (Archives) and Configuration folder (by default,* ***C:\Proficy Historian Data****).*

15. Accept the default Historian Archives folder or browse for a new location and, then click Next. The Configuration Review screen appears.
16. Click Next.

17. Select '**Yes, I want to restart my computer now**", and then click Finish to complete the installation.

Log Files Created After You Start Historian for the First Time

When you start collection, the Historian Server creates an archive. It places archive files in the **Archives** folder specified during installation. By default, this is **C:\Proficy Historian Data\Archives** on both 32-bit and 64-bit Windows operating system. All files with the .IHA extension are Archive data files. The file with the .IHC extension contains configuration information.

The archiver and collectors place log files in the **Logfiles** folder. By default, this is **C:\Proficy Historian Data\LogFiles** on both 32-bit and 64-bit Windows operating system. The Archiver produces two log files, a *DATAARCHIVER-XX.LOG* file and a *DATAARCHIVER.SHW* file. Each collector also produces two log files. For example, the Simulation Collector produces these files: SimulationCollector-01.log and SimulationCollector.shw.

You can view log files using Notepad or any other text editor. The .LOG file shows events, warnings, and errors produced by the Archiver during operation; the .SHW file shows current configuration information that applies to the Historian Server.

Installing Historian Non-Web Administrator

You can install an Historian Non-Web Administrator on any node that connects to the Server through an Historian API.

To install an Historian Non-Web Administrator:

1. Insert the **Historian** DVD. The Historian splash screen appears.

   NOTE: *If this screen does not automatically appear, double-click the InstallFrontEnd.exe file on the DVD to display it. A message may appear with a security warning; click Run to proceed.*

2. Click the "**Historian Installer**" link. A message box appears asking you to confirm the install.
3. Click **Run** to proceed. The install program starts and the **Welcome** screen appears.
4. When the Install Wizard appears, select the **Historian Administrator** option in addition to any previously installed Historian components, and then click **Next**.

   The program installs the Historian Non-Web Administrator and any other components associated with it, including the API. If you prefer, you can install the Historian Administrator at the same time you install other options, by selecting all desired options at once.

NOTE: *If you intend to run all components (Historian Server, Collectors, and Client tools) on a single computer, choose Historian Installer on the splash screen and proceed with the installation wizard.*

Starting the Historian Non-Web Administrator

To start the Historian Non-Web Administrator:

1. From the **Start** button in the bottom toolbar, select **Program Files** and then **Proficy Historian 5.5**.
2. Select **Historian Administrator** to open the application.

   As an alternative, you can create a shortcut and start Historian from a desktop icon.

3. Optionally, click on the **Main** link. The login dialog box appears.
4. Optionally, select the server from the drop-down menu, enter your **username**, **password**, and **domain**, if any, and then click **OK**.

   The Historian System Statistics screen appears. You can now proceed with all Historian Administrator functions.

   NOTE: *If you leave the* ***UserName****,* ***Password****, and* ***Domain*** *fields blank and click* ***OK****, then the login information of the currently logged in Windows user is used.*

Installing Historian Data Collectors

All collectors, except the iFIX and Machine Edition* View collectors can run as Windows services. If so configured, they will also continue to run after you log out, and can be configured to start when you start your computer. The iFIX Collector, on the other hand, starts when iFIX or FIX starts, and runs after logout if iFIX or FIX is so configured.

You can install only one Server-to-Server Collector and one Calculation Collector per computer.

NOTE: *Historian data collectors must be installed after the source software has been installed. For example, the iFIX SCADA software must be installed before the iFIX collector. Wherever possible, data collectors should be installed on the same machine as the data source, to take maximum advantage of collector buffering.*

Steps to Install Data Collectors

NOTE: *If you intend to run all components (Historian Server, Collectors, and Client tools) on a single computer, click* ***Historian Installer*** *on the splash screen and proceed with the installation wizard.*

To install Historian Data Collectors :

1. Insert the Historian DVD. The Historian splash screen appears.

NOTE: *If this screen does not automatically appear, double-click the InstallFrontEnd.exe file on the DVD to display it. A message may appear with a security warning; click Run to proceed.*

2. Click the "**Historian Collectors**" link. A message box appears asking you to confirm the install.
3. Click Run to proceed. The install program starts and the Welcome screen appears.
4. Select the appropriate type of Data Collector in addition to any previously installed Historian components, and then click **Next**. The Choose the Program Folder screen appears.
5. Accept the default destination folder or browse for a new location, and then click Next. The Historian Server Name screen appears.

   NOTE: *On a 64-bit Windows Operating System, the default destination folder for all 32-bit components (such as collectors and APIs) is* ***C:\Program Files\Proficy\Proficy Historian\x86*** *directory. Similarly, for all 64-bit components (such as Excel Add-in 64-bit and SQL Server 64-bit), it is installed in* ***C:\Program Files\Proficy\Proficy Historian\x64*** *directory.*
6. Enter the Historian Server name to be used, and then click Next. The Configuration Review screen appears.

   NOTE: *Historian now creates Log files and Buffer files folder inside Data (Archives) and Configuration folder (by default,* ***C:\Proficy Historian Data****).*
7. Click Next.
8. Select '**Yes, I want to restart my computer now**", and then click Finish to complete the installation.

NOTE: *The collector will not appear in the Historian Administrator until after the collector has been started.*

Installing the Historian Excel Add-In

You can install the Excel Add-In on any client or server on which the API has been installed.

NOTE: *If you intend to run all components (Historian Server, Collectors, and Client tools) on a single computer, click* ***Historian Installer*** *on the splash screen and proceed with the installation wizard.*

To install the Excel Add-In:

1. Verify that Microsoft Excel is installed on your computer.
2. Insert the Historian DVD. The Historian splash screen appears.

   NOTE: *If this screen does not automatically appear, double-click the InstallFrontEnd.exe file on the DVD to display it. A message may appear with a security warning; click Run to proceed.*

3. Click the "**Historian Excel Add-in**" link. A message box appears asking you to confirm the install.
4. Click Run to proceed. The install program starts and the Welcome screen appears.
5. Click Next to proceed. The License Agreement screen appears.
6. Click Yes to continue. The Select Features screen appears
7. Select the component that you want to install, and then click Next. The Choose the Program Folder screen appears.
8. Accept the default destination folder or browse for a new location, and then click Next. The Historian Server Name screen appears.

   NOTE: *On a 64-bit Windows Operating System, the default destination folder for all 32-bit components (such as collectors and APIs) is* ***C:\Program Files\Proficy\Proficy Historian\x86*** *directory. Similarly, for all 64-bit components (such as Excel Add-in 64-bit and SQL Server 64-bit), it is installed in* ***C:\Program Files\Proficy\Proficy Historian\x64*** *directory.*

9. Enter the Historian Server name to be used, and then click Next. The Configuration Review screen appears.
10. Click Next.
11. Select '**Yes, I want to restart my computer now**", and click Finish.

If you prefer, you can install the Excel Add-In at the same time you install a data collector or server. The Add-In must be enabled in Excel before you can use it. To enable the Excel Add-In, refer to Installing the Excel Add-In with Historian in the Using the Historian Excel Add-In manual.

Installing the Historian Client Tools

NOTE: *If you intend to run all components (Historian Server, Collectors, and Client tools) on a single computer, click* ***Historian Installer*** *on the splash screen and proceed with the installation wizard.*

To install the Client Tools:

1. Insert the Historian DVD. The Historian Splash screen appears.

   NOTE: *If this screen does not automatically appear, double-click the InstallFrontEnd.exe file on the DVD to display it. A message may appear with a security warning; click Run to proceed.*

2. Click the "**Historian Client Tools**" link. A message box appears asking you to confirm the install.
3. Click Run to proceed. The install program starts and the Welcome screen appears.
4. Click Next to proceed. The License Agreement screen appears.

5. Click Yes to continue. The Select Features screen appears.
6. Select the component that you want to install, and then click Next. The Choose the Program Folder screen appears.
7. Accept the default destination folder or browse for a new location, and then click Next. The Historian Server Name screen appears.

   NOTE: *On a 64-bit Windows Operating System, the default destination folder for all 32-bit components (such as collectors and APIs) is* ***C:\Program Files\Proficy\Proficy Historian\x86*** *directory. Similarly, for all 64-bit components (such as Excel Add-in 64-bit and SQL Server 64-bit), it is installed in* ***C:\Program Files\Proficy\Proficy Historian\x64*** *directory.*

8. Enter the Historian Server name to be used, and then click Next. The Configuration Review screen appears.
9. Click Next.
10. Select '**Yes, I want to restart my computer now**", and then click Finish to complete the installation.

Installing the Historian HDA Server

IMPORTANT: *You must install Historian Non-Web Administrator to setup the Proficy Historian OPC HDA Server.*

You can install the Proficy Historian OPC HDA Server on any server on which the Proficy Historian Server has been installed.

To install the HDA Server:

1. Insert the Historian DVD. The Historian splash screen appears.

   NOTE: *If this screen does not automatically appear, double-click the InstallFrontEnd.exe file on the DVD to display it. A message may appear with a security warning, click Run to proceed.*

2. Click the "**Historian Installer or Historian Client Tools**" link. A message box appears asking you to confirm the install.
3. Click Run to proceed. The install program starts and the Welcome screen appears.
4. Click Next to proceed. The License Agreement screen appears.
5. Click Yes to continue. The Select Features screen appears
6. Select the component (HDA Server) that you want to install, and then click Next. The Choose the Program Folder screen appears.

7. Accept the default destination folder or browse for a new location, and then click Next. The Historian Server Name screen appears.

   NOTE: *On a 64-bit Windows Operating System, the default destination folder for all 32-bit components (such as collectors, client tools, and APIs) is* ***C:\Program Files\Proficy\Proficy Historian\x86*** *directory. Similarly, for all 64-bit components (such as Excel Add-in 64-bit and SQL Server 64-bit), it is installed in* ***C:\Program Files\Proficy\Proficy Historian\x64*** *directory.*

8. Enter the Historian Server name to be used, and then click Next. The Configuration Review screen appears.
9. Click Next.
10. Select '**Yes, I want to restart my computer now**", and click Finish to complete the installation.

NOTE: *When the HDA Server option is selected, then the Historian install wizard will install Microsoft .NET Framework 3.5 and OPC Core Components 3.00 redistributable during the installation process.*

Installing Historian SDK

If you need to create customized programming for the Historian Server, use the Historian Software Development Kit (SDK) with Visual Basic or any application that provides a VBA programming interface, such as iFIX, Microsoft Excel or Microsoft Word. The Install Wizard places the Historian Software Development Kit (SDK) in the System32 directory and automatically registers it. To use the SDK, set up a project reference with the Proficy Historian Software Development Kit.

Installing Historian Client Access API

For Microsoft.Net based application development, use the Historian Client Access API with C#, VB.Net, or any .Net compliant application. By default, the Install Wizard places both the API and Client Access dlls in GAC (Global Assembly Cache). If you want to reference it to any client application, you can refer the following file path: ”INSTALLPATH\Assembly\Proficy.Historian.ClientAccess.API.dll”.

IMPORTANT: *It is recommended that you add Historian Client Access API references from INSTALLPATH directory since global assembly cache is part of the run-time environment.*

Uninstalling Historian and Historian System Components

To remove all Historian System information from your computer:

1. Double-click the Add/Remove Programs icon in the Control Panel. The Add/Remove Programs dialog box opens.
2. Select Proficy Historian, and click the **Remove** button.
    a. To uninstall Historian and save the current Historian configuration and data, select **Do Not Delete Archives** and click **Next**.
    b. To uninstall Historian and delete the current Historian configuration and data, select **Delete Archives** and click **Next**.
    c. To abort the uninstall, select **Cancel Uninstall** and click **Next**.
3. The uninstall proceeds and all Historian components are removed.

For information on uninstalling OPC Data Collectors, refer to the Modifying and Uninstalling OPC Collectors section of the Historian Data Collectors manual.

Upgrading from a Previous Release

Before upgrading Historian, it is recommended that you follow these steps:

- Stop the Historian Data Archiver service.
- Backup all archive data files (*.iha), configuration files (*.ihc) and backup files. By default, in Proficy Historian 3.5 or earlier you can find these files in the *C:\Program Files\GE Fanuc\Proficy Historian\Archives* folder.
- Optionally, use the Excel Add-In to export your tag configuration for all tags. It is recommended that you export tags associated with each collector on a separate worksheet.
- If you are using Microsoft Excel 2000, then you must upgrade to Microsoft Excel 2003 or above.
- If you are using a SQL Server 2000 database, then you must:
    - Stop the Historian Services including the Alarm Archiver service.
    - Upgrade to SQL Server 2008 or higher before upgrading Historian.
    - Upgrade to Historian 5.5. During the Install process provide the valid connection information to the SQL Server 2008.
- Shut down the DEP (Data Execution Protection) feature. One way to do this is from the Control Panel,

access the System Properties. Select the Advanced tab, and click the Settings button in the Performance area. On the Data Execution Protection tab, select the "Turn on DEP for essential Windows programs and services only" check box.

NOTE: *Hardware-enforced DEP is always enabled for 64-bit native programs such as the Proficy Historian Data Archiver. Setting DEP to apply to "Essential Windows Programs only" will not disable DEP for the Data Archiver but, depending on your configuration, hardware-enforced DEP may be disabled for 32-bit programs such as the Calculation Collector.*

To determine whether your computer's processor supports hardware-enforced DEP or not, contact the manufacturer of your computer.

If you upgrade to Historian 5.5, then you must upgrade your Historian license key to Historian 5.5. Check the Historian SIM download page for any available updates and install them as part of your upgrade.

Uninstalling the old Historian Product

You can uninstall the old Historian product before installing the new Historian, but you do not have to. If you choose to uninstall, make sure that you remove all Historian SIMs before uninstalling the old Historian product.

If you uninstall the old Historian product, you do not need to remove any Historian archives, unless you want to. When you use the **Windows Add Remove Programs** wizard to uninstall Historian, a message box appears asking if you want to remove the archives. If upgrading, select the **Do Not Delete Archives and Continue** option and click **Next** to continue with the uninstall.

Installing the new Historian Product

If you chose to uninstall Historian first, make sure you restart your computer before installing the new Historian. For the steps on how to install Historian, refer to the section at beginning of this chapter, Installing Historian Software.

NOTE: *If you have uninstalled a previous version of Proficy Historian and did not remove the archives, ensure you direct the new Historian to the previous install folder (for example, C:\Program Files\GE Fanuc\Proficy Historian\Archives\ ) so that the Historian install program will find the existing archives and configuration file.*

The default installation folder will now reflect the new Proficy name. By default, Proficy Historian 5.5 installs to:

C:\Program Files\Proficy\Proficy Historian

The archives, log files, and buffer files are installed to these locations:

C:\Proficy Historian Data\Archives

C:\Proficy Historian Data\BufferFiles

C:\Proficy Historian Data\LogFiles

The help files are installed to:

C:\Program Files\Proficy\ProficyDoc\1033\Historian

Proficy Historian Server now supports 64-bit environment. For a 64-bit environment, this support covers the native 64-bit Historian server. You can also install Historian Collectors, Client tools, APIs, and Non-Web Administrator on 64-bit Windows operating systems, but Collectors, Client tools, APIs, and Non-Web Administrator, and works as a 32-bit applications on a 64-bit Windows operating system using WoW64 mode (Windows-on-Windows 64-bit). However, you can read and write data from a 64-bit Historian Server.

On a 64-bit Windows Operating System:

- The default destination folder for a 64-bit Historian Server is *C:\Program Files\Proficy\Proficy Historian\x64\Server* directory.
- The default destination folder for all 32-bit components (such as collectors, APIs and so on) is *C:\Program Files\Proficy\Proficy Historian\x86* directory.
- The default destination folder for all 64-bit components (such as Excel Add-in 64-bit and SQL Server 64-bit) is *C:\Program Files\Proficy\Proficy Historian\x86* directory.
- The default archives, log files, and buffer files are installed to *C:\Proficy Historian Data*.
- The help files are installed to *C:\Program Files\Proficy\ProficyDoc\1033\Historian*.
- When you are upgrading Historian 3.5 or earlier and if you did not remove the archives, ensure you direct the new Historian to the previous install folder (for example, *C:\Program Files\GE Fanuc\Proficy Historian\Archives*) so that the Historian install program will find the existing archives and configuration file.

NOTE: *On a 64-bit Windows Operating System, all 32-bit components (such as collectors, client tools, and APIs) related registry keys will be located under HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\\Intellution, Inc.\iHistorian\.*

Upgrading the Historian SDK

If you want to run an SDK program that you created with an older version of Historian on a newer version, you must first rebuild the program on a computer with the new version installed. You must build the SDK application built on the Historian version you will be running the program on.

Migration Tool

The IHA migration tool Migrateiha.exe allows you to migrate data up to 30 years old if the data is already stored in IHA files from any version of Historian. Use the MigrateIHA.exe program to move data from one archiver to another when you cannot simply restore the IHA in the Historian Administrator.

Migrateiha.exe opens an IHA file as a binary data file and reads the raw samples from it. Then those raw samples are written to a destination archiver similar to how an OPC collector or File Collector would write data. Any errors returned from the data archiver will be reported in the main window and repeated in the log file.

Using Migration Tool

The following procedure describes how to migrate historical data stored in IHA files from any version of Historian.

***NOTE**: You need to run this tool as an administrator to migrate and create the log files in the C:\.*

To Migrate Historical data using the MigrateIHA tool

1. In Historian folder, click the MigrateIHA.exe Button, shown in the following figure, to open the IHAMigration Utility.

- MigrateIHA.exe Button

2. Select Configure Options from the Options menu.
3. Enter or modify any specific configuration information. For more information, refer to the Configuring Migration Options section.
4. Select Migrate Historical Data from the File menu. The Select Historical Data File(s) dialog box appears.
5. Select a historical file and click Open.

Refer to the IHA Migration Utility main screen for information on the progress of the migration and any encountered errors.

***NOTE**: The IHA Migration Utility screen only displays the most recent lines of the log file. For the full set of logged messages, refer to the log file, typically located in C:\IHAMigration.Log.*

To Bulk Upgrade Historical Data

You can upgrade the older versions archive files to the latest version by selecting this option. If you do a Bulk Upgrade of Historical Data immediately after you installed the latest version on Proficy Historian, then you would save on the upgradation while the system reboots.

To Bulk upgrade Historical Data, stop the Data Archiver service and select the Bulk Upgrade Historical Data from the File menu.

To Clear the Display

To clear the log messages displayed in the screen, select the Clear Display from the File menu.

To View the Log File

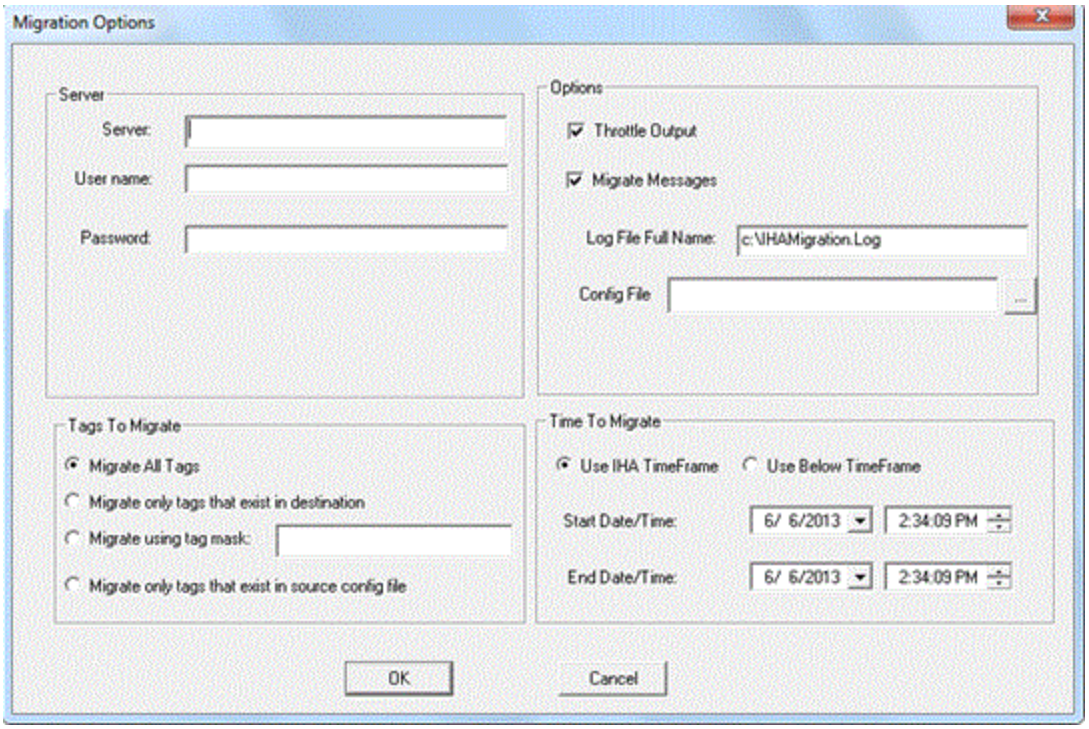
To view the logs saved in the IHAMigration.log file, select the View Log File from the File menu.

Configuring Migration Options

Open the Migration Options dialog box, shown in the following figure, by selecting Configure Options from the Options menu in the MigrateIHA.exe Utility.

The MigrateIHA Tool automatically detects the default server and displays the default migration options. Some of the options that you can configure include:

- Server Section
- Options Section
- Tags to Migrate Section
- Time to Migrate Section



Server Section

This section allows you to set up your server information.

The Historian Server Options include:

Field	Description
Server	The default server (set during installation). If you do not want to write data to the default server, enter the desired server in this field.
Username and Password	If you have created and established Security Groups in your Historian Security Environment, you may need to enter the user name and password here. By default, if you do not supply any information, the current logged in user will be used in security checking. For more information about Historian Security, please refer to the Implementing Historian Security chapter.

Options Section

This section allows you configure the options for data migration. The Option section includes:

Field	Description
Throttle Output	Select this option to throttle any part of the migration process. Optionally, you can remove this option as required. By default throttling is rated at 5000 events per second. ***NOTE**: If you select this option, the migration might be a bit slow.*
Migrate Messages	Select this option to migrate the messages into the newly created archive. Using this option may or may not reduce the size of your archives, depending on the number of messages stored in the archive. By default, messages are migrated.
Log File Full Name	Modify the location of the IHAMigration.log.
Config File	The configuration (*.IHC) file which you want to migrate. You must provide the IHC file before selecting an IHA file. ***TIP**: It is always advisable to take a copy of the configuration file and work on the copy rather than working on the original file.*

Tags to Migrate Section

This section gives you different options to migrate the tags in the case where you do not want to migrate data for all tags.

Option	Description
Migrate All Tags	Select this option to migrate all the tags from the selected archiver.
Migrate only tags that exist in destination	Select this option to migrate all the tags that exists in the source destination.

Migrate using tag mask	Select this option to migrate tags with the mask specified. You can specify an exact tag name to migrate that tag only.
Migrate only tags that exist in source config file	To migrate the tags that are present only with the source config file.

Time to Migrate Section

Use this section to specify the time frame for migration if you want to migrate only a subset of the data.

Option	Description
Use IHA TimeFrame	Select this option to migrate all the tags which has the IHA time frame.
Use Below TimeFrame	Select this option to migrate all the tags in the specified time frame. You need to specify the Start Date/Time and End Date/Time if you select the this option.

Command-line Options for the IHA Migration Tool

Command line options for the IHA Migration tools are:

- **/NOTHROTTLE** - This does not throttle any part of the migration process, but may impact resources on the server. Optionally, you can remove this switch as required. By default throttling is rated at 5000 events per second.
- **/NOMESSAGES** - This does not migrate messages into the newly created archive. Using this switch may or may not reduce the size of your archives, depending on the number of messages stored in the archive. By default, messages are migrated if this switch is not used.
- **/EXISTINGTAGS** - This will migrate data for only those tags that exist in the destination archiver.
- **/b** - This option of the start.exe file allows the IHA Migration tool to start without opening a new window for each instance.
- **/wait** - This option of the start.exe file allows each instance of the IHA Migration tool to complete the migration before starting the next migration in the sequence.
- **/b** - If you are migrating a pre 4.5 IHA file you will need to have the IHC file for that IHA and specify

the IHC file in the Options dialog or on the command line. Otherwise, you will get a warning message.

If you do not have the IHC or you are not sure you have the correct IHC then you should use the pre 4.5 version of MigrateIHA to migrate the IHA.Otherwise the data will not migrate correctly. The IHC must contain all the tags that are in the IHA file so use the most current IHC you have. Migrating an IHA will upgrade it to 4.5 format. You should keep a copy of the original IHA file. If you are migrating from a command line you must provide the IHC filename as in this example The syntax to run the MigrateIHA.exe tool at command line is: MigrateIHA.exe “IHA file name with full path” “IHC filename with full path” If you are migrating a 4.5 IHA you should provide the IHC file in the options dialog but if you do not have the IHC you can safely continue past the warning message.

To Write a Batch File to Migrate Multiple IHA Files using Migrate IHA

- The IHA Migration utility will migrate only one archive at a time by design. As a result, if you are required to add more than one archive at a time, you can create a batch file to automate multiple archive merges.

***TIP**: When migrating any archive, you should start with the archive with the oldest data first, followed by later times in sequence to minimize the amount of disk space used in the Data Archiver.*

You can migrate multiple IHA files through a batch file. While creating a batch file you need to provide the batch file with a logical name and save the batch (.bat) file in a location which could be easily accessed using command prompt. For example:

```
cd c:\Program Files\Proficy\Proficy Historian
start /b /wait migrateiha /NOTHROTTLE /NOMESSAGES "c:\Proficy Historian
Data\Backups\server_Archive001.iha" "c:\Proficy Historian
Data\Backups\server_Config.ihc"
```

***NOTES**:*

- *If you are using Proficy Historian 5.5 or above, during Migrate IHA, you need to pass the IHC file.*
- *You should have double quotes when you enter the IHA and IHC file even if you do not have spaces in your file path or file name.*

Interoperability of Historian Versions

Interoperability guidelines for Historian versions include:

- Historian Collectors below v5.1 can write to Historian v5.1 Archivers.

- Historian Clients below v5.1 can retrieve data from Historian v5.1 Archivers.
- Historian v5.1 Clients can retrieve data from Historian Archiver below v5.1.
- Historian v5.1 Collectors can write to Historian Archivers below v5.1.
- An SDK program built on an Historian v5.1 node does not run on an Historian below v5.1.
- An SDK program that you created in Historian below v5.1 must be rebuilt on a computer with Historian v5.1 if you want to run it on the v5.1.
- In general, it is recommended that you use consistent versions of client and server applications. If you do use different client and server versions of the Historian, it is recommended to regularly back up all archives and tag configurations.

  NOTE: *To determine the version of the server, client, and SDK, click on the About link in the Historian Administrator.*

Troubleshooting

FAQ About Upgrading to Historian 5.5

Question	Answer
How do I upgrade Historian 3.1 SP1 or above to Historian 5.5?	You can upgrade Historian 3.1 SP1 or above using the Historian 5.5 full installer only.
How do I upgrade Historian versions earlier than 3.1 SP1 to Historian 5.5?	You must un-install the version earlier than Historian 3.1 SP1, and then install Historian 5.5.
How do I upgrade Historian 3.0 or 3.1 which is installed on Windows 2000 or Windows XP SP2 operating system?	You must upgrade to Windows XP Professional SP3, Windows Server 2003 SP 2, Windows Vista SP1 32-bit (Business, Ultimate, and Enterprise), Windows Server 2008-32 bit, or Windows 2008 Server 64bit Edition (WoW64). ***NOTE:*** *Historian is not supported on Windows 2000 or Windows XP operating system.*

How do I upgrade Historian 3.1 which contains FIX32 and CIMPLICITY native collectors?	You must un-install Historian 3.1or later which contains FIX32 and CIMPLICITY native collectors and then install Historian 5.5. ***NOTE:*** *Historian 5.5 does not support FIX32 and CIMPLICITY native collectors.*
How do I upgrade Historian 3.1 which uses Microsoft Excel 2000?	You must install Microsoft Excel 2003 or later and then install Historian 5.5. ***NOTE:*** *Historian 5.5 does not support Microsoft Excel 2000 and Excel XP.*
How do I upgrade Historian 3.1 which uses SQL Server 2000 database ?	If you are using a SQL Server 2000 database then you must: • Stop the Historian Services including the Alarm Archiver service. • Upgrade to Historian 5.5. During the Install process provide the valid connection information to the SQL Server 2008. ***NOTE:*** *Historian 5.5 does not support SQL Server 2000.*
Do I need to install a SQL Server Express 2008 and then migrate MSDE data into SQL Server Express 2008?	No. Historian 5.5 Installer will install SQL Server Express 2008 and migrate the MSDE data into SQL Server Express 2008 automatically.
How do I upgrade Historian 3.1 or later which contains server, collectors, and client tools using components installer; for example, collectors only or client tools only, or excel add-in only installers?	You must use Historian 5.5 full installer only.

How do I upgrade Historian 3.1 or later Collectors using Historian 5.5 Collectors install only?	You must use either Historian 5.5 full installer or Collectors only installer to upgrade. ***NOTE:*** *If an individual component (for example, collectors only or client tools only, or excel add-in only) of Historian 3.1 is installed on a machine, then you must use either Historian 5.5 full installer or an individual component installer to upgrade.*
Does Historian 5.5 support Proficy Historian Server in native 64-bit?	Yes. You can now install "Proficy Historian 5.5 Server" on both 32-bit x86 systems and 64 bit "x64" systems. Historian 5.5 installer will automatically detect and install 32-bit or 64-bit Historian 5.5 Server based on system architecture.
Does Historian 5.5 support Historian Collectors and Non-Web Administrator in native 64-bit?	No. You can install Historian Collectors, Non-Web Administrator, works on 64-bit Windows operating systems, but they work as a 32-bit application on a 64-bit Windows operating system using WoW64 mode (Windows-on-Windows 64-bit).
Does Historian 5.5 support 64 bit SQL server?	Yes, one of the following 32-bit or 64-bit SQL Server systems to configure alarm and event archiving: • Microsoft SQL Server 2008 Standard, Professional, or Enterprise Edition. • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 Express.
Does Historian 5.5 supports 64 bit SQL linked server?	Yes. You can use one of the following 64-bit versions of SQL Server to use Historian as a linked server: • Microsoft SQL Server 2008 Standard, Professional, or Enterprise Edition. • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2005 Standard SP2, Professional SP2, or Enterprise Edition SP2. • Microsoft SQL Server 2008 Express.

Does Historian 5.5 support 64-bit Microsoft Excel Add-In?	Yes. Historian 5.5 supports Microsoft 2010 64-bit Excel Add-in.
Can I create 64-bit SDK applications?	No.
Can I use User API applications (such as, CollectorLike, PlotLike, ReportLike, and MigrationLike) to read and write data to a 64-bit Historian server?	Yes. Historian allows you to use the User API applications (such as, CollectorLike, PlotLike, ReportLike, and MigrationLike) to read and write data to a 64-bit Historian server.
Can I write 64-bit Visual Basic ado applications to OLEDB?	No.

Implementing Historian Security

Historian is a high performance data archiving system designed to collect, store, and retrieve time-based information efficiently. By default, access to these Historian archives, tags, and data files is available to any valid operating system user account. In this default environment, all users are allowed to read, write, change, and delete archives, tags, or data files in the Historian Administrator, SDK, Migration Tools, and Excel Add-In. However, you may find that you want to make these functions and data available only to authorized personnel. You can do this by creating and defining Historian Security Groups in your Windows Security.

Historian includes an Electronic Signature and Electronic Records security feature. This option provides installations concerned with the FDA's 21 CFR Part 11 regulation – or any site interested in added security or tracking – the ability to require a signature and password every time a change in data or configuration is requested. For more information on the Electronic Signature and Electronic Records feature, refer to the Using Historian in a Regulated Environment section of the Using the Historian Administrator manual.

Whether or not you use Historian security, make sure that you disable Guest accounts on your computer to limit access to valid Windows user accounts.

Protecting Your Process

If you want to restrict access to Historian archives, files, and tags, or protect your data files from unauthorized changes, you can enable Historian security. Using security is optional and is disabled by default. By enabling security, you can restrict access to the following:

- Modifying data using the Excel Add-In
- Updating security for individual tags or groups of tags
- Creating, modifying, and removing tags

  Tag protection (adding, modifying, removing, an so on) can be applied at a global level to all tags or at the individual tag level. Refer to Implementing Tag Level Security for more information.

- Reading data in the iFIX Chart object, Excel Add-In, and Migration Utilities
- Writing data
- Starting and stopping collectors
- Creating and deleting collectors
- Creating, modifying, and deleting archives

Historian uses the operating system security groups to create a security structure. You enable security for a particular set of functions by adding specific Historian Security Groups to your groups. You can also add security groups to your domain controller. Refer to Security Tab section in the Historian Administrator Manual for information on selecting local or domain security groups.

By defining one or all of the groups, you begin to set up a security structure. Refer to the Historian Security Groups section for more information on the Historian Security Groups available.

Implementing Strict Authentication

With Proficy Historian's strict user account authentication features, Enforce Strict Client Authentication and Enforce Strict Collector Authentication, you can control access to the Historian server and safeguard user account credentials.

With strict authentication enabled, only known user accounts configured on the Data Archiver server computer will be able to access a Historian server. Similarly, enabling strict collector authentication enforces the same requirement for incoming collector connections.

For an account to be known at the Data Archiver, it has to exist on that archiver as a local account or exist on a Domain Controller available to the data archiver. Historian will access the local accounts or Domain Controller

via Microsoft's Security Support Provider Interface (SSPI) and this involves having a Kerberos server setup optionally to assist in account validation.

By default, strict client and collector authentication is enabled on new installations to maximize security. When upgrading from a previous version of Historian, strict client and collector authentication is disabled to allow compatibility with older clients or collectors that cannot be upgraded concurrently.

It is recommended that all clients and collectors receive timely upgrade to the latest version, which permits enabling both strict client and collector authentication on the server for the highest security configuration.

By treating clients and collectors separately, it is possible to accommodate new and legacy authentication during the upgrade process. However, upgrading all clients and collectors to the latest version immediately will achieve a high level of security. The two options, Enforce Strict Client Authentication and Enforce Strict Collector Authentication, permit flexibility during the upgrade process by selectively accommodating legacy clients and/or collectors.

The following table enumerates a guideline about the different combinations of strict client and collector authentication options and their use:

Strict Authentication Options		
Authentication		
Strict Client	**Strict Collector**	**Comment**
Enabled	Enabled	Use this for highest available security. You will need to install SIMs, if available on all pre-5.5 collectors and clients. Clients can refer to any program that connects to the Data Archiver. This includes Historian Administrator, Microsoft Excel, any OLEDB program, user written programs, or any other Proficy software.

Enabled	Disabled	Use this if you are unable to upgrade collectors to the latest version if there is no SIM update for your collector.
Disabled	Enabled	Use this if you have to support legacy clients and you are unable to install SIM update on all clients.
Disabled	Disabled	Use this for maximum compatibility with existing systems.

For more information, refer to the product IPI (Important Product Information) e-book or SIM release notes.

Disabling Strict Client or Collector Authentication

To permit older versions of clients and collectors to access a Historian 5.5 server, disable strict client and collector authentication.

To disable strict client and collector authentication:

1. Open the DataStore Maintenance screen, click the Security tab.
2. In the Global Security section:
    - Select the Disabled option button for Enforce Strict Client Authentication option.
    - Select the Disabled option button for Enforce Strict Collector Authentication option.

Troubleshooting Strict Authentication Issues

If the Proficy Historian Server rejects valid collector or client user credentials while connecting, consider the following conditions:

Windows XP computer rejects valid credentials when accessing the Historian server with strict authentication enabled

If a Windows XP (SP3) computer that is a member of a work group is rejecting valid credentials while trying to access a server with strict authentication enabled, it means that the ForceGuest registry value is set to 1 by

default, in the registry key. Use the following steps to choose the correct option:

1. Open the Control Panel, and then from the Administrative Tools, select Local Security Policy, Local Policies, and then Security Options.
2. Go to Network access, and then Sharing and security model for local accounts.
3. Set the **Classic - local users authenticate as themselves** option.

Time Sync between the Server Time and Domain Controller Time

If a client or collector is attempting to connect to the Historian server with Strict Authentication enabled on a Kerberos configuration, ensure that the Server's and Domain Controller's time match with each other. Otherwise, the server rejects valid credentials and does not allow the connection.

Creating and Implementing a Security Strategy

When you begin to implement security, you should first define a clear strategy. Consider the following when beginning to set up your security strategy:

- If you disabled the Guest account, a user must provide a valid username and password even if no groups are created.
- Protection is only provided for the functional areas for which you have built the associated Historian Security Groups.
- If you only choose to define some of the security groups, all users still have all access to any uncreated groups. All users are still assumed to be a member of a group unless that group has been created, with the exception of iH Audited Writers group. You must add the iH Audited Writers group to the Windows security groups so that a user can become a member of this group.

  For example, if you elect to define the iH Security Admins group and iH Archive Admins group, both the members associated with those defined groups and all other valid users still have access to such functions as creating and modifying tags until you create the iH Tag Admins security group.

- If you decide to implement any of the Historian Security groups, you should first add and define the iH Security Admins group.

  WARNING: *If you do not create and define the iH Security Admins group, all valid users are assumed to be members of this group. This membership overrides any other security group that you set.*

For more information on the Historian Security Groups available and their security functions, refer to the Historian Security Groups section and the Historian Security Groups table.

Historian Login Security

Use Historian Login Security settings if you want to validate users at the Data Archiver, instead of at the client. By applying these settings, users and applications will be forced to provide a user name and password at connect time so that archiver can validates them. For example, users in the security group such as "ih Security Admins" will be checked by the Archiver.

For Historian Login Security settings, you can view and set the property from the HistorianSDKsample server properties. The current setting is shown in the data archiver SHW file.

Historian Login Security property is available only in Historian SDK.

To set login security using the Historian SDK:

1. Run the SDK sample.

2. Connect to a server.

3. Double-click on the server from the list box, The Server Properties dialog box appears.

4. On the right side of the dialog box, locate the AllowClientValidation setting. By default, this value is set to TRUE. Click to set to FALSE, and then, click OK.

Historian Security Groups

The following are the available Historian Security groups:

iH Security Admins – Historian power security users. Security Administrators have rights to all Historian functions. This group also has the ability to change tag level security, archive security, and modify the Electronic Records and Signatures option. This is the only Historian security group that overrides tag level security.

iH Collector Admins – Allowed to start and stop collectors, browse collectors, configure collectors, and add new collectors.

iH Tag Admins – Allowed to create, modify, and remove tags. Tag level security can override rights given to other Historian security groups. Tag Admins can also browse collectors.

iH Tag Admins are not responsible for setting Tag Level Security. This task can only be performed by an iH Security Admins. For more information on setting Tag Level Security, refer to the Implementing Tag Level Security section.

iH Archive Admins – Allowed to create, modify, remove, backup, and restore archives.

iH UnAudited Writers – Allowed to write data without creating any messages.

iH UnAudited Logins – Allowed to connect the DataArchiver without creating login successful audit messages.

iH Audited Writers – Allowed to write data and to produce a message each time a data value is added or changed.

Tag, archive, and collector changes log messages regardless of whether the user is a member of the iH Audited Writers Group.

iH Readers – Allowed to read data and system statistics. Also allowed access to Historian Administrator.

Historian Group Rights

Use the security table that follows to identify which types of user groups you need to create and define in your security system.

Historian Security Groups

Function	**iH Security Admins**	**iH UnAudited Writers**	**iH UnAudited Login**	**iH Audited Writers**	**iH Readers**	**iH Archive Admins**	**iH Tag Admins**	**iH Collector Admins**
Create Tags: • Excel Add-In • SDK • Historian Administrators • File Collector	**X**						**X**	
Remove Tags: • Historian Administrators • SDK • File Collector	**X**						**X**	

Modify Tags: • Historian Administrators • Excel Add-In • SDK • File Collector	**X**						**X**	
Modify Archive Security: • Historian Administrators • SDK	**X**							
Backup Archive: • Historian Administrators • SDK	**X**					**X**		

Restore Backup: • Historian Administrators • SDK	**X**					**X**		
Create Archive: • SDK • Historian Administrators	**X**					**X**		
Start/Stop Collector: • SDK • Mission Control (iFIX) • Historian Administrators	**X**							**X**
Browse Collector: • Historian Administrators	**X**							**X**

Read Data: • Chart Object • Excel Add-In • SDK	**X**				**X**			
Write Data (UnAudited): • Excel Add-In • SDK	**X**	**X**	**X**					
Write Data (Audited): • Excel Add-In • SDK	**X**			**X**				
Modify Data: • Excel Add-In • SDK	**X**	**X**	**X**	**X**				

Update Security for Tag: • Excel Add-In • SDK • Historian Administrators	**X**							
Migrate • Migration Tools	**X**							
Login Connection Messages	**X**	**X**		**X**	**X**	**X**	**X**	**X**

Security Setup Example

The following example takes you through the process of establishing your security needs and defining and setting up the levels of security.

Example

This example demonstrates how to implement security with Historian, starting with the default open security system.

1. Establish your user needs.

   For this example, assume the following user needs in a plant of 14 users:

User	Needs	Added to Security Group
USER1	Power user. Needs total access to security.	iH Security Admins
USER2 USER3 USER5 USER6 USER8	• Read/Write Data (no messages). • Create, modify, and delete tags. • Backup, restore, and create archives. • Connect to DataArchiver without creating login successful audit messages	• iH UnAudited Writers • iH Tag Admins • iH Archive Admins • iH UnAudited Logins
USER4 USER7	• Read/Write Data (no messages). • Create, modify, and delete tags. • Start/Stop Collectors. • Backup, restore, and create archives.	• iH UnAudited Writers • iH Tag Admins • iH Collector Admins • iH Archive Admins
USER9-14	Read Data.	• iH Readers

2. Add and define the iH Security Admins Group.

   Once you determine that you want to establish a security structure, you must create and define the iH Security Admins group. This group of users is typically the "power users" of the Historian. Security Administrator rights allow them to manage configuration and give them free rein to the entire system. For this example, only USER1 would be added to the iH Security Admins group.

3. Establish and create any other Historian Security Groups as needed.

   NOTE: *Any user with Windows administrative permissions can add or remove Windows groups and users. As such, an administrator on a Windows computer, can add himself to any Historian security group.*

   You should then set up the functional security groups as needed. For this example, Write, Tag,

Archive, and Collector security is required, so the groups associated with those functions should be added and defined. There is no need for Audited Writers and all valid users can read data, so neither the iH Audited Writers Group nor the iH Readers Group need to be added.

4. Define any individual Tag Level security.

   In addition to defining iH Tag Admins that have the power to create, modify, and remove tags, you can also define individual tag level security to restrict access to sensitive tags. You can grant read, write, or administrative privileges per tag. For more information on setting Tag Level security, refer to the Implementing Tag Level Security section.

Setting up Historian Security Groups

This section describes how to add the Historian Security Groups to your local and domain Windows security systems.

You can choose whether Historian uses LOCAL or DOMAIN security by selecting an option on the Security Tab of the Data Store Maintenance screen in the Historian Administrator. If you select the local security option, the groups are defined as local groups on the Historian Server. If you select the Domain security option, the groups are defined as global groups in the primary domain controller of the Historian Server. With domain security, Historian locates the Primary Domain Controller (PDC), if available, or a Backup Domain Controller (BDC) in order to establish groups. If the PDC and all BDCs are unavailable, the system locks all users out until rights can be established with a valid PDC or BDC.

NOTE: *If you change this setting, you must stop and re-start the Historian Server for this change to take effect.*

Setting Local Groups on Windows Systems

The following procedures applies setting local groups on a Windows XP® Professional with Service Pack2 or 3 (32-bit); Windows Vista® (32-bit and 64-bit); Windows Server® 2003, 2008, and 2008 R2; or Windows 7 (32-bit and 64-bit).

To create a new local group:

1. Open the Control Panel.
2. Double-click the Administrative Tools.
3. Double-click the Computer Management icon. The Computer Management console opens.
4. Select Groups from the Local Users and Groups folder in the system tree.
5. From the Action menu, select New Group. The New Group dialog box appears.

6. Enter the Historian Security Group name in the Group Name field. For a list of available Historian Security Groups and their functions, refer to the Historian Security Groups section.

   IMPORTANT: *You must enter the Historian Security Group name exactly as it appears. The security groups are case sensitive.*

7. Optionally, enter a description of the Historian Security Group in the Description field.
8. Click Create.
9. Click Close.

Adding Users to Windows Security Group

Before adding users to your group, you must first add your users to the Windows system. For more information on adding users, refer to the Users Overview section of the Windows 2003 or XP Pro online Help.

To add a user to a group:

1. Open the Control Panel.
2. Double-click the Administrative Tools icon.
3. Double-click the Computer Management icon.
4. Select Groups from the Local Users and Groups folder in the system tree.
5. Select the group to which you want to add users.
6. From the Action menu, select Properties. The Users Properties dialog box appears.
7. Click Add.
8. Select the users or groups to add from the listed users or enter the names of the users or groups you want to add in the bottom field.
9. Click Add.

   TIP: *To validate the user or group names that you are adding, click Check Names.*

10. When you have added all users to the group, click OK.

To add a local user:

1. Verify object types is Users or Groups.
2. Verify the From This Location setting is your local machine. (Click Locations to specify the local machine, if required.)
3. Click Advanced. The Advanced dialog box appears.

4. Click Find Now.
5. From the list of users, select the users or groups to add or enter the names of the users or groups you want to add in the bottom field.
6. In the Advanced dialog, click OK.
7. In the Select Users dialog, click OK.
8. In the group properties dialog, click OK.

To Add a Domain User:

1. Verify object types is Users or Groups.
2. Verify the From This Location setting is your windows domain.
    a. Click Locations to specify the domain, if required.
    b. Select Entire Directory or the specific domain underneath Entire Directory.
    c. Click OK
3. Click Advanced. The Advanced dialog box appears.
4. Click Find Now.
5. From the list of users, select the users or groups to add or enter the names of the users or groups you want to add in the bottom field.
6. In the Advanced dialog, click OK.
7. In the Select Users dialog, click OK.
8. In the group properties dialog, click OK.

Avoiding Unauthorized Access When Using Historian Security

To ensure a secure environment when using Historian security, do not create any local user accounts unless Historian is set up on a stand alone machine. Also, disable the Windows Guest account.

Working with Domain Security

When you configure Historian to use Domain security groups, the Data Archiver attempts to locate the groups on the Primary Domain Controller (PDC) or one of the Backup Domain Controllers (BDC). If you don't have primary domain controller or if it is slow to access, you can have the Data Archiver access the nearest domain controller via the UseADSICalls registry key. When using a PDC, if a Primary or Backup Domain Controller cannot be located when the Historian Data Archiver service starts, access to Historian is denied to all users.

For troubleshooting, the data archiver show (.SHW) file lists all PDCs and BDCs available at the time of archiver startup. Use this list to verify that the Historian Server has visibility into the appropriate domain.

When using a PDC, after the list of Domain Controllers has been established, the Historian Server will use that list to query for Security Group Membership on an as needed basis. If at any time a request for Group Membership information is made and the Primary Domain Controller is not available, Historian selects the first Backup Domain Controller and attempts the same request. If a Backup Domain Controller successfully responds to the request, the process of querying for Group Membership can stop. Otherwise, Historian will attempt to query Group Membership information from the next available Backup Domain Controller. If no Backup Domain Controller successfully responds, access to the system is denied.

When using UseADSICalls registry key, Historian does not connect to a specific domain controller and lets the operating system contact the most available one.

Changing security group configuration from Local to Domain or vice versa requires that the Historian Data Archiver service be restarted for the change to take effect.

Creating Security Groups in Windows 2003 Domain Controller

To create a new Global security group in a Windows 2003 Domain:

1. In the Control Panel, double-click Administrative Tools. The Administrative Tools dialog box opens.
2. Double-click the Active Directory Users and Computer icon. The Active Directory dialog box opens.
3. In the Active Directory Tree display, select the required Domain and select Users.
4. Right-click Users, select New and then click Group. The New Object - Group dialog box appears.
5. In the Group name field, enter the name of the new Historian group exactly as you have defined it. Leave the other default options unchanged.
6. Click OK to create the new group.

Creating Security Groups in Windows 2008 Domain Controller

To create a new security group in a Windows 2008 Domain:

1. In the Control Panel, double-click Administrative Tools. The Administrative Tools dialog box opens.
2. Double-click the Active Directory Users and Computer icon. The Active Directory dialog box opens.
3. In the Active Directory Tree display, select Users.
4. Right-click Users, select New and then click Group. The New Object - Group dialog box appears.
5. In the Group name field, enter the name of the new Historian group exactly as you have defined it.

Leave the other default options unchanged.

6. Click OK to create the new group.

Using a Windows 2003 Domain Controller with a Windows 2008 Historian Server

When you use domain security with a Windows 2008 Historian Server and the domain controller is a Windows 2003 controller, you must configure the Historian DataArchiver service to log on as a valid domain account and you must add the user right. To Act as a Part of the Operating System to its list of rights.

To set up logon of Historian data archiver service

1. In Control Panel > Administrative Tools, double-click Services. The Services dialog box opens.
2. Double-click Historian Data Archiver. A Service dialog box appears.
3. In the Log On As panel, click This Account and select a domain user account.
4. Click OK.

To add the *Act As Part of Operating System* right to the domain account

1. In Administrative Tools, double-click Domain Security Policy. The Default Domain Security Settings dialog box appears.
2. In the Security Settings tree, select User Rights Assessment from Local Policies .
3. Double-click Act as a part of the operating system policy. The Act as a part of the operation system dialog box appears.
4. Select Define these policy settings check box, and then click Add User or Group button. The Add Users and Groups dialog box appears.
5. Select your domain username.
6. Click Add and then click OK.
7. In Services, restart Historian DataArchiver.

   You should now be able to log on to Historian Administrator using Domain Security.

If you attempt to log on to the Historian Data Archiver as a Local System Account, you may be denied access because the System Account in Windows 2008 is not privileged to access the Windows 2003 Domain

Administrator. A valid domain user account, however, is privileged to access the Windows 2003 Domain Administrator if it is has also been granted the Act as a Part of the Operating System right.

Configuring DataArchiver to use Active Directory Service Interface

By default, the DataArchiver tries to enumerate all the available domain controllers during startup. If a Primary or Backup Domain Controller cannot be located when the Historian DataArchiver service starts, access to Historian is denied to all users. Also when you have domain controller machines spread across a wide area network (WAN), you may find that logins are successful but slow.

With the Active Directory Support feature, you can configure the DataArchiver to use a different set of Windows calls called Active Directory Services Interface (ADSI) when using Historian security. Configuring the DataArchiver to use Active Directory Services Interface (ADSI) allows you to:

1. Login to the Historian even if the DataArchiver is unable to enumerate any domain controllers during the DataArchiver startup.
2. Access a Backup Domain Controller if a Primary Domain Controller is not available temporarily or permanently.

You should configure the DataArchiver to use Active Directory Services Interface (ADSI) only when the DataArchiver fails to enumerate domain controllers.

You can determine whether or not the DataArchiver is able to locate a domain controller by viewing the dataarchiver.shw log file. In the dataarchiver.shw log file If **“Group Server #01:** “is empty, then the DataArchiver is unable to locate a domain controller.

```
Security Settings

=================

                          Group Mode : GLOBAL

   Use Client Windows User for Logon : TRUE

                     Security Domain : <your domain>

                    Group Server #01 :
```

*N**OTE:** You must run the DataArchiver under an account with domain administrator privileges to use Active Directory Services Interface either temporarily or permanently.*

The following procedures provide guidelines for configuring the DataArchiver to use Active Directory Services Interface (ADSI) calls.

Creating a registry key and turning on the UseADSICalls

1. On the Start menu, click Run. (For Windows Vista, Windows Server 2008, and Windows 7, click the Windows Start button and click inside the Start Search field)
2. Type Regedit and click OK. The Registry Editor dialog box opens.
3. Open the following key folder HKEY_LOCAL_MACHINE\SOFTWARE\Intellution, Inc.\Historian\Services\DataArchiver\
4. Add a new DWORD value. Enter the name “UseADSICalls”, and select Base as Decimal.
5. In the Value data field, type 1.
6. Click OK.
7. Close the Registry Editor and configure the DataArchiver service to run as domain administrator.

Configuring the DataArchiver service to run as domain administrator

1. On the Start menu, click Run. (For Windows Vista, Windows Server 2008, and Windows 7, click the Windows Start button and click inside the Start Search field).
2. Type services.msc and click OK. The Services dialog box opens.
3. Right-click the Historian DataArchiver service and select Properties.
4. Click the Log On tab, and then select the Log on as This account to log on special account.
5. Click the Browse button and select the user account.
6. In the Password and the Confirm password fields, enter the password for the user account, and then click OK.

Restart the DataArchiver service

1. On the Start menu, click Run. (For Windows Vista, Windows Server 2008, and Windows 7, click the Windows Start button and click inside the Start Search field).
2. Type services.msc and click OK. The Services dialog box opens.
3. Right-click the Historian DataArchiver service and click Restart.

Reviewing the .SHW log file

The DataArchiver log file is used to examine the current configuration of a DataArchiver. The default path for LOG and SHW files is **C:\Proficy Historian Data\LogFiles**.

If the DataArchiver is set correctly to use Active Directory Services Interface (ADSI), then you can find the

following text in the DataArchiver.SHW log file

```
Security Settings
=================
                          Group Mode : GLOBAL
   Use Client Windows User for Logon : TRUE
                    Security Domain : <your domain>
                     Use ADSI calls : TRUE
```

Establishing Your Security Rights

Your security identity is established upon connecting to the server. This occurs through the following steps:

1. Specifying a username and password of an account.

   Upon connection, the system checks to see if you have a valid Windows 2003 account. If you have supplied a username and password (through the Excel Add-In for example), security checks that user. If username and password are not supplied and you are on a Windows 2003 or Windows 2008 machine or higher, security checks the currently logged in user.

   NOTE: *If you do not pass a domain name the account will be checked locally in the same way a mapped drive attempt happens. You have to specify a username and password that exists on the server.*

2. Determining group membership of that account.

   Once the account is validated, the server determines group membership. For more information on the process and hierarchy of the groups, refer to the Identifying the Security Checking Process section.

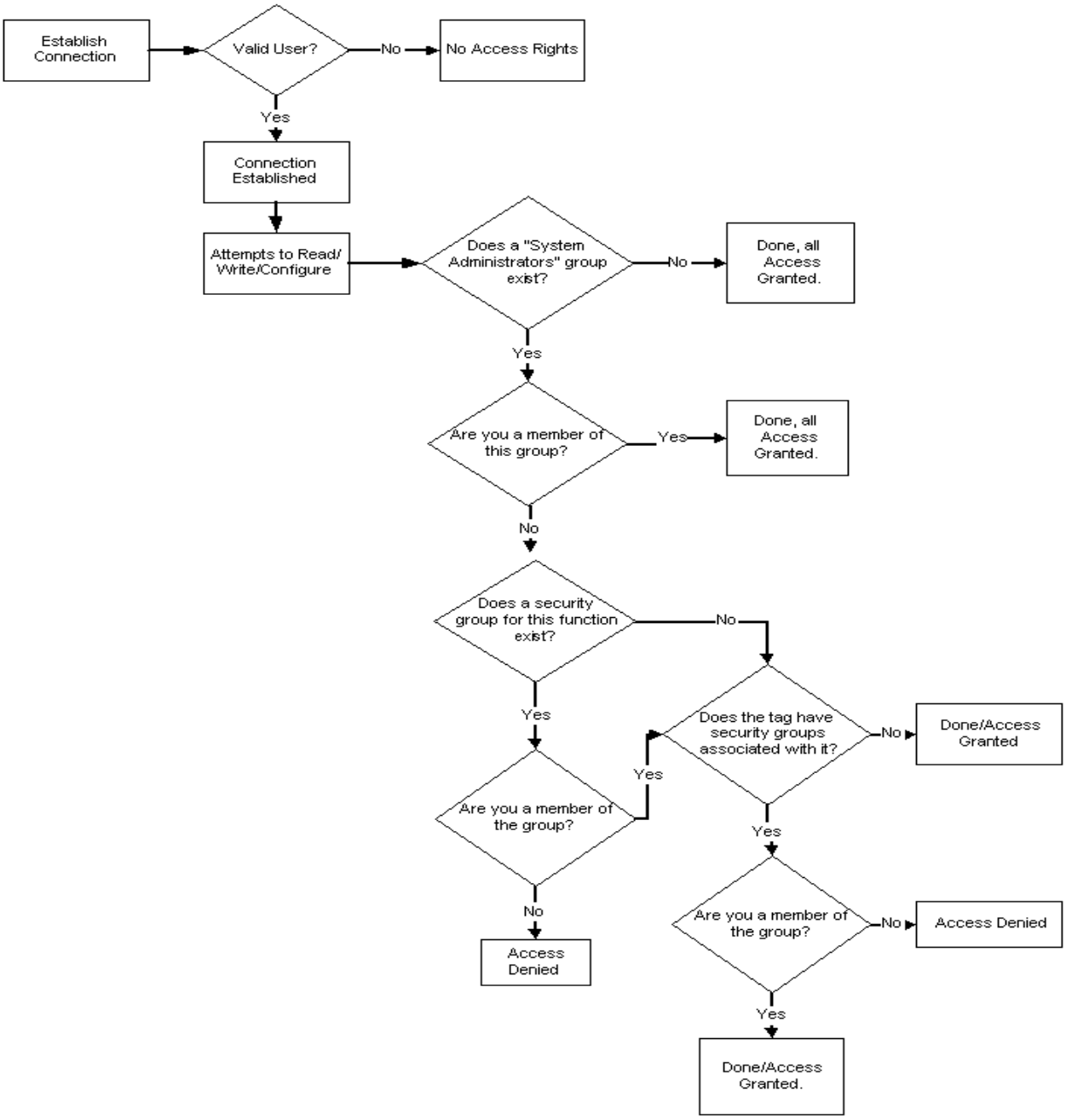
3. Caching membership profile.

   Once the group and tag membership are determined, it is cached for the connection and not looked up again. If users are added to or deleted from a group, the cache is not updated.

   NOTE: *The cache information is per connection, and not per IP address. In other words, it is cached per application and not per system.*

Identifying the Security Checking Process

The following figure details the security checking process.



Security Checking Process

Implementing Tag Level Security

In addition to defining iH Tag Admins that have the power to create, modify, and remove tags, you can also define individual tag level security to protect sensitive tags.

This tag level security can be set in the Historian Administrator. You do not need to use the Historian Security Groups for this security setting. You may use one of the Windows pre-defined groups (power users, for example) or create your own separate group specifically for this function. For more information on creating and adding groups, refer to the Setting up Historian Security Groups section.

NOTE: *Only users defined as iH Security Admins have rights to set individual tag level security, browse and query all tags in the Historian Administrator*.

To set Tag Level Security for an individual tag:

1. Open the Historian Administrator.
2. Click on the Tags link. The Tag Maintenance screen appears.
3. Select a tag (or group of tags) from the Tag Name section of the Tag Maintenance screen.
4. Click on the Advanced Tab to display the advanced tag options.
5. In the Read Group, Write Group, or Administer Group field, select the security group that you wish to assign to the tag from the drop-down list.

   The drop-down list automatically lists all security groups that are defined in your Windows security environment.

For example, if an iH Security Admins user selects a tag and chooses power users from the Read Group drop-down list, in addition to members of the iH Security Admins group, only a member of the power users group will be able to read data for that tag. Even a member of the iH Readers group will not be able to access data for that tag, unless they are also defined as a member of the power users group.

Retrieving Data from Historian

After data collection, the Historian Server compresses and stores the information in the Archive Database. Any client application can retrieve archived data through the Historian API. The Historian API is a client/server programming interface that maintains connectivity to the Historian Server and provides functions for data storage and retrieval in a distributed network environment.

You can retrieve data from Historian using one of the following:

- iFIX
- CIMPLICITY
- Excel Add-In
- Custom SDK Applications
- OLE DB
- API
- Charting

Sampling and calculation modes are used on retrieval of data that has already been collected to the archive. These modes do not effect data collection. Some sampling modes are suited to compressed data and should be used when collector compression or archive compression is used.

Sampling Modes

Sampling modes are used to specify how the data will be retrieved from Historian. Several modes are available, such as CurrentValue, Interpolated, Calculated and RawByTime. Sampling modes are specified in the client you use to retrieve data from Historian.

For more information, refer to the Advanced Topics section in the online help.

Descriptions and common usages of the sampling modes in Historian are as follows:

Sampling Mode	**Results**
CurrentValue	Retrieves the most recent data sample value received by the archiver, of any data quality. This does not necessarily produce the most recent raw data sample, as archive compression may not have stored the most recent raw sample. The sample has a time stamp, a value, and a quality. The time stamp returned is not typically the current time; it is the time stamp as sent by the collector. If you have a slow poll rate or if collector compression is enabled, the time stamp may be much earlier than the current time.

RawByTime	Returns all raw samples of all qualities with a time stamp greater than a specified start time, and less than or equal to a specified end time. The RawByTime sampling mode will not return a sample equal to the start time.
RawByNumber	Returns a specified number of samples of all qualities with a time stamp greater than or equal to the start time. The RawByNumber sampling mode will return a sample with a time stamp equal to the start time if one exists You must also specify a direction and number of samples when using this sampling mode.
Interpolated	When archive or collector compression is used, a minimal number of actual data samples are stored in the archive. When this data is retrieved, interpolation can be performed to create an evenly spaced list of most likely real-world values (since the actual values have been removed from the archive through the compression algorithm). The Interpolated sampling mode is also useful for data samples that haven't undergone archive compression. For example, you may want to plot data along an interval that doesn't match the collected raw samples. Using the Interpolated sampling mode would give you the most likely real-world values for the specified period. Typically, you use the interpolated sampling mode when data is not collected on a set time schedule, or if you want to see the results returned in an interval that is slower than the collection rate. For example, these instances show when you can use interpolated mode to make evenly spaced values: • A tag is collected as "unsolicited." In this case, we really do not know what the time interval is between collected values. • The deadband and/or archive compression for a tag results in non-evenly spaced collection intervals. • A tag is collected once per 8-hour shift, but you want to see it displayed in 1 hour intervals with a linear slope between points.

InterpolatedtoRaw	When you request interpolated data, you specify an interval or number of samples. If the actual stored number of raw samples is greater than required, you will get interpolated data as described above. If the actual number of stored samples are less than the required, then you will get the raw samples. In this way, the needs of trending detail and application load are balanced. This mode is best used when querying compressed data because the Data Archiver can switch to the more efficient raw data query.
Lab	The Lab sampling mode only returns the collected values, without any interpolation of the value. The collected value is repeated for each interval until there is a change in the raw data sample's value. Lab sampling is most often used to create a step chart rather than a smooth curve. Use Lab sampling instead of interpolated if you only want true collected values returned. The Lab sampling mode is generally not useful on highly compressed data. Use interpolated sampling instead.
LabtoRaw	LabtoRaw is an extension to Lab mode of sampling and similar to InterpolatedtoRaw mode where you will be switched to raw data or lab when the actual data samples are fewer than the requested samples.
Trend	The Trend sampling mode was designed to produce maximum performance when retrieving data for plotting, particularly over long time periods. The trend sampling mode returns the maximum and minimum value collected during each interval. When plotted, this makes it possible to display an accurate representation of the data that won't miss any extremums, by only retrieving a minimum of points. For example, a trend of 1 year of data with a 1 day interval will return 730 values consisting of the 365 minimums and 365 maximums for each day of the year.

TrendtoRaw	TrendtoRaw retrieves raw data between a given intervals when the actual data samples are fewer than the requested number of samples.
Calculated	Returns samples based on a selected Calculation mode. Refer to Calculation Modes for more information.
RawByFilterToggle	RawByFilterToggle returns filtered time ranges. The values returned are 0 and 1. If the value is 1, then the condition is true and 0 means false. This sampling mode is used with the time range and filter tag conditions. The result starts with a starting time stamp and ends with an ending timestamp

Calculation Modes

Calculation modes are used when the sampling mode is set to Calculated. The data type of all calculated values will be DoubleFloat except for MinimumTime, MaximumTime, FirstRawTime and LastRawTime which will be a Date. The datatype of the values of FirstRawValue and LastRawValue will be the same as that of the selected tag.

The calculation modes in Historian are:

Calculation Mode	**Results**
Count	Displays the number of raw samples in the specified interval. This only indicates the count and does not display the actual values or qualities of the samples. The Count calculation mode is useful for analyzing the distribution of raw data samples. If you have a higher number of raw samples than expected, you may decide to implement collector or archive compression. If samples are missing then you may want to slow your collection rates

State Count	Displays the number of times a tag has transitioned to another state from a previous state. A state transition is counted when the previous good sample is not equal to the state value and the next good sample is equal to state value.
State Time	Displays the duration that a tag was in a given state within an interval.
Minimum	Displays the minimum value in a specified interval with good data quality. This value may be raw or interpolated. ***NOTE:*** *The Minimum and MinimumTime calculation retrieve two additional samples per interval; one is interpolated at the interval start time and the other is interpolated at the interval end time. These samples are used to determine the min or max just like any raw value.*
MinimumTime	Displays the time stamp of the minimum value in a specified interval. See the note in Minimum for additional information.
Maximum	Displays the maximum value in a specified interval. ***NOTE:*** *The Maximum and MaxmimumTime calculation internally retrieve two additional samples per interval; one is interpolated at the interval start time and the other is interpolated at the interval end time. These samples are used in the min or max just like any raw or interpolated value.*
MaximumTime	Displays the time stamp of the maximum value in a specified interval. See the note in Maximum for additional information.

RawAverage	Displays the arithmetic average of the raw values in a specified interval with good data quality. This is useful only when a sufficient number of raw data values are collected.
Average	Similar to RawAverage, but performs a special logic for time weighting and for computing the value at the start of the interval. This is useful for computing an average on compressed data.
OPCQOr and OPCQAnd	The OPCQOr is a bit wise OR operation of all the 16 bit OPC qualities of the raw samples stored in the specified interval. The OPCQAnd is a bit wise AND operation of all the 16 bit OPC qualities of the raw samples stored in the specified interval.
Total	Retrieves the time-weighted total of raw and interpolated values for each calculation interval. The collected value must be a rate per 24 hours. This calculation mode determines a count from the collected rate.
RawTotal	Displays the arithmetic sum of raw values in a specified interval.
StandardDeviation	Displays the time-weighted standard deviation of raw values for a specified interval.
RawStandardDeviation	Displays the arithmetic standard deviation of raw values for a specified interval.
TimeGood	Displays the amount of time (in milliseconds) during an interval when the data is of good quality and matches filter conditions if the filter tag is used.

FirstRawValue	Returns the first good raw value for a specified time interval.
FirstRawTime	Returns the timestamp of the first good raw for a specified time interval.
LastRawValue	Returns the last good raw value for a specified time interval.
LastRawTime	Returns the timestamp of the last good raw for a specified time interval.
TagStats	Using TagStats, you can return multiple calculation modes for a tag in a single query.

***NOTE**: You can also use INCLUDEBAD or FILTERINCLUDEBAD as query modifiers to include bad quality data. For more information, refer INLUDEBAD and FILTERINCLUDEBAD sections in Advance Topics.*

Query Modifiers

Query Modifiers are used for retrieving data that has been stored in the archive. They are used along with sampling and calculation modes to get a specific set of data. The following are the available query modifiers in Proficy Historian.

For more information, refer to the Query Modifiers section.

Descriptions and common usages of Query Modifiers in Historian are as follows:

Query Modifier	Results
ONLYGOOD	The ONLYGOOD modifier excludes bad and uncertain data quality values from retrieval and calculations. Use this modifier with any sampling or calculation mode but it is most useful with Raw and CurrentValue queries. All the calculation modes such as minimum or average exclude bad values by default, so this modifier is not required with those.
INCLUDEREPLACED	Normally, when you query raw data from Proficy Historian, any values that have been replaced with a different value for the same timestamp are not returned. The INCLUDEREPLACED modifier helps you to indicate that you want replaced values to be returned, in addition to the currently retrievable data. However, you cannot query only the replaced data and the retrievable values that have replaced other the values. You can query all currently visible data and get the data that has been replaced. This modifier is only useful with rawbytime or rawbynumber retrieval. Do not use it with any other sampling or calculation mode.

INCLUDEDELETED	The INCLUDEDELETED modifier retrieves the value that was previously deleted. Data that has been deleted from the archiver is never actually removed but is marked as hidden. Use the INCLUDEDELETED modifier to retrieve the values that were deleted, in addition to any non-deleted values during the query time period. This modifier is only useful with rawbytime or rawbynumber retrieval. Do not use it with any other sampling or calculation mode.
ONLYIFCONNECTED/ONLYIFUPTODATE	The ONLYIFCONNECTED and ONLYIFUPTODATE modifiers can be used on any sampling or calculation mode to retrieve bad data if the collector is not currently connected and sending data to the archiver. The bad data is not stored in the IHA file but is only returned in the query. If the collector reconnects and flushes data and you run the query again, the actual stored data is returned in the following situations: • Collector loses connection to the archiver • Collector crashes • Collector compression is used and no value exceeds the deadband

ONLYRAW	The ONLYRAW modifier retrieves only the raw stored samples. It does not add interpolated or lab sampled values at the beginning of each interval during calculated retrieval such as average or minimum or maximum. Normally, a data query for minimum value will interpolate a value at the start of each interval and use that together with any raw samples to determine the minimum value in the interval. Interpolation is necessary because some intervals may not have any raw samples stored. Use this query modifier with calculation modes only, not with raw or sampled retrieval like interpolated modes.
LABSAMPLING	The LABSAMPLING modifier affects the calculation modes that interpolate a value at the start of each interval. Instead of using interpolation, lab sampling is used. When querying highly compressed data you may have intervals with no raw samples stored. An average from 2 P.M to 6 P.M on a one hour interval will interpolate a value at 2 P.M., 3 P.M., 4 P.M, and 5 P.M and use those in addition to any stored samples to compute averages. When you specify LABSAMPLING, then lab sampling mode is used instead of interpolated sampling mode to determine the 2 P.M., 3 P.M., 4 P.M., and 5 P.M., values. A lab sampled average would be used when querying a tag that never ramps but changes in a step pattern such as a state value or setpoint. Use this query modifier with calculation modes only, not raw or sampled retrieval like interpolated modes.

ENUMNATIVEVALUE	The ENUMNATIVEVALUE modifier retrieves the native, numeric values such as 1 or 2 instead of string values such as on/off for the data that has enumerated states associated with it. You can use ENUMNATIVEVALUE with any sampling or calculation mode.
INCLUDEBAD	Normally, when you query calculated data from Proficy Historian, only good data quality raw samples are considered. INCLUDEBAD modifier includes bad data quality values in calculations. You can use INCLUDEBAD with any sampling or calculation mode.
FILTERINCLUDEBAD	Typically while filtering we use only good data quality values. When we use FILTERINCLUDEBAD, the bad data quality values are considered when filtering to determine time ranges. This query modifier is not always recommended.
USEMASTERFIELDTIME	The USEMASTERFIELDTIME query modifier is used only for the MultiField tags. It returns the value of all the fields at the same timestamp of the master field time, in each interval returned.

Filtered Data Queries

Filtered data queries enhance Historian by adding filter tags and additional filtering criteria to standard queries. Unfiltered data queries in Historian allow you to specify a start and end time for the query, then return all data samples within that interval. A filtered data query, however, will allow you to specify a condition to filter the results by, as well as calculation modes to perform on the returned data. Filtered data queries are performed on the Historian server.

For example, a filtered data query is useful when trying to retrieve all data for a specific Batch ID, Lot Number, or Product Code and for filtering data where certain limits were exceeded, such as all data where a temperature exceeded a certain value. Rather than filtering a full day's worth of process data in the client application, you can filter data in the Historian archiver, and only return the matching results to the client application. The result is a smaller, more relevant data set.6.00975/5.

You can use filter criteria with raw, interpolated, and calculated sampling modes. You cannot use it with current value sampling. The logic of selecting intervals is always interpolated, even when the data retrieval is raw or calculated. The value that triggers a transition from false to true can be a raw value or interpolated value.

You cannot use a filtered data query in an iFIX chart. For more information, refer to Advanced Topics section in the online help.

Overview of Filtered Data Query Parameters

Use of filter parameters with a data query is optional. The following table describes each of the filtering parameters you can use.

Filter Parameters for Data Queries

Parameter	Description
Filter Tag	The single tag name used when applying the filter criteria. ***NOTE**: You can enter your filter conditions using Filter tag, Filter Comparison Mode, and Filter Comparison Value or you can put that all that information in a single FilterExpression.*

Filter Expression	An expression which includes one or more filter conditions. The type of conditions used are: • AND Condition • OR Condition • Combination of both AND and OR Filter Expression can be used instead of FilterTag, FilterComparisonMode and FilterValue parameters. While using FilterExpression, the expression is passed within single quotes and for complex expressions we write the conditions within a parenthesis. There is no maximum length for a filter expression, but if it is called using OLEDB or Excel, they may have their own limitations.
Filter Mode	The type of time filter: • **ExactTime** – Retrieves data for the exact times that the filter condition is True (only True). • **BeforeTime** – Retrieves data from the time of the last False filter condition up until the time of the True condition (False until True). • **AfterTime** – Retrieves data from the time of the True filter condition up until the time of next False condition (True until False). • **BeforeAndAfterTime** – Retrieves data from the time of the last False filter condition up until the time of next False condition (While True). The Filter Mode defines how time periods before and after transitions in the filter condition should be handled. For example, AfterTime indicates that the filter condition should be True starting at the timestamp of the archive value that triggered the True condition and leading up to the timestamp of the archive value that triggered the False condition.

Filter Comparison Mode	***NOTE**: Filter Comparison Mode is only used if Filter Tag is filled in.* The type of comparison to be made on the filter comparison value: • **Equal** – Filter condition is True when the Filter Tag is equal to the comparison value. • **EqualFirst** – Filter condition is True when the Filter Tag is equal to the first comparison value. • **EqualLast** – Filter condition is True when the Filter Tag is equal to the last comparison value. • **NotEqual** – Filter condition is True when the Filter Tag is NOT equal to the comparison value. • **LessThan** – Filter condition is True when the Filter Tag is less than the comparison value. • **GreaterThan** – Filter condition is True when the Filter Tag is greater than the comparison value. • **LessThanEqual** – Filter condition is True when the Filter Tag is less than or equal to the comparison value. • **GreaterThanEqual** – Filter condition is True when the Filter Tag is greater than or equal to the comparison value. • **AllBitSet** - Filter condition is True when the binary value of the Filter Tag is equal to all the bits in the condition. It is represented as ^ to be used in Filter Expression. • **AnyBitSet** - Filter condition is True when the binary value of the Filter Tag is equal to any of the bits in the condition. It is represented as ~ to be used in Filter Expression. • **AnyBitNotSet** - Filter condition is True when the binary value of the Filter Tag is not equal to any one of the bits in the condition. It is represented as !~ to be used in Filter Expression. • **AllBitNotSet** - Filter condition is True when the binary value of the Filter Tag is not equal to all the bits in the condition. It is represented as !^ to be used in Filter Expression. • **Alarm Condition** – Specifies an alarm condition to filter data by. For example, *Level*. • **Alarm SubCondition** – Specifies an alarm sub-condition to filter data by. For example, *HIHI*. The Filter Comparison Mode defines how archive values for the Filter Tag should be compared to the Filter Value to establish the state of the filter condition. If a Filter Tag and Filter Comparison Value are supplied, time periods are filtered from the results where the filter condition is False.

Filter Comparison Value	***NOTE**: Filter Comparison Value is only used if Filter Tag is filled in.* The value to compare the filter tag with when applying the appropriate filter to the data record set query (to determine the appropriate filter times).

Example: Filtered Queries in the Excel Add-In

The following example shows how a filtered data query will return specific data from the Historian archive.

This example makes use of two tags, **batchid** and **ramp**. The **batchid** tag is updated before a new batch is produced with the new batch's ID. The **ramp** tag contains raw data sent by a device in the process. In this example, we'd like Historian to return data samples at ten second intervals for the **ramp** tag during the period that the **batchid** tag is set to *B1*.

A standard query in Historian for the ramp tag's values between 08:00 and 08:01, at ten second intervals, would look like this:

Time Stamp	**Value**	**Data Quality**
07/30/2003 08:00:10	16	Good
07/30/2003 08:00:20	22	Good
07/30/2003 08:00:30	34	Good
07/30/2003 08:00:40	46	Good
07/30/2003 08:00:50	50	Good
07/30/2003 08:01:00	55	Good

If we did a query against the batchid tag for the same time interval, we would receive the following results:

Time Stamp	Value	Data Quality
07/30/2003 08:00:00	B0	Good
07/30/2003 08:00:20	B1	Good
07/30/2003 08:00:45	B2	Good

To filter data queries in the Excel Add-in:

In order to find the values of the ramp tag for the B1 batch, you would enter the following values into the Historian Filtered Data Query dialog box:

1. In the **Tag Name(s)** field, enter the tag you want to receive results from - the ramp tag in this example.
2. Select a start and end time for your query.
3. In the **Filter Tag** field, enter the tag you want to enable filtering with - *batchid* in this example.
4. In the **Filter Comparison** field, select your comparison condition.
5. In the **Include Data Where Value Is** field, enter your filter condition value.
6. In the **Include Times** field, select your filter mode.
7. In the **Sampling Type** field, select your sampling mode.
8. In the **Calculation** field, select your calculation mode.
9. Select your **Sampling Interval.**
10. In the **Output Display** field, select which tag values you wish to display.

NOTE*: You can enter your filter conditions using Filter tag, Filter Comparison Mode, and Filter Comparison Value or you can put that all that information in a single FilterExpression. You can enter the filter conditions in the* ***FilterExpression*** *field of the Historian Data Query dialog box. The filter conditions are passed within single quotes.*

Using Historian with iFIX

You can enhance the power of the Historian by pairing it with iFIX. The benefits of using Historian with iFIX clients include:

- iFIX Chart features:
  - Sub-second support
  - Auto Update
  - Time Zone Support
  - Daylight Savings Time (DST) Support
  - Filter and Sort by description, and directly access OPC tags in the Expression Editor
  - Support for Historian interpolated data retrieval.
- Ability to access multiple Historian Servers (even within the same chart).
- The ability to easily script against the SDK in VBA. This allows you to retrieve record sets in Historian for processing and display, and to build time-aware graphics that can display animations from any selected time.
- Writing status information directly into iFIX tags, so the health of the iFIX Collector can be monitored in real time within iFIX.
- Easy migration of iFIX Classic Historian Configuration and Data.
- Easy migration of iFIX Alarm and Event Data.
- Collection of iFIX Alarm and Event Data.

NOTE: *You can plot any collected data, not just iFIX Collector data.*

Please be aware of the following when using Historian with iFIX:

- You must install iFIX before installing Historian if you want to install the iFIX Collector. If you attempt to install Historian on a machine without iFIX installed and select the iFIX Collector under the Select Components, a message appears stating that iFIX is required on this node to install the iFIX Collector.
- You must install the iFIX Alarm & Event server before installing the iFIX AE Collector from the Historian installation and setup program.
- You must manually import the Historian Toolbar into the iFIX WorkSpace after you have installed Historian. Refer to Importing the Historian Toolbar into iFIX for more information.

- In working with iFIX, be aware that the Historian security is independent of iFIX security.
- If you attempt to use the iFIX Chart Group Wizard to add Simulation or OPC tags, you will receive an error. The Chart Group Wizard only supports iFIX Historian tags that use the iFIX historical tag naming convention.
- Historian does not support the installation of collectors or servers on Terminal Server machines running in application server mode.

Using iFIX drivers with Historian

If you are running iFIX in your Historian environment, you can use any iFIX driver (version 6.X or 7.X). Historian uses data from the iFIX process database, therefore once the driver brings the data into the Process Database (PDB), it is available to Historian via EDA and the iFIX Collector.

Collecting iFIX Alarm and Event Data

Historian supports Alarm and Event collection from an iFIX server.

To configure the iFIX AE collector to start automatically when iFIX starts add the iFIX AE collector to the list of startup tasks in the System Configuration Utility (SCU).

To add the collector to the SCU list, open the **Task Configuration** dialog box in iFIX, enter *ihIFIXAECollector.EXE* in the **Filename** field and *runasdos* in the **Command Line** field, and click the **Add** button.

NOTES:

- *After starting the iFIX AE collector you will need to use the Historian administration tool to link it to its associated iFIX data collector.*
- *If ItemIDs are not being collected, and you see an entry in your log file that says "Alarm Item IDs Will Not Be Collected. 'CV' Vendor Attribute Not Found", you must increase the Delay Collection at Startup (sec) value in the collector's configuration.*

For more information, refer to the following topic:

- OPC Alarm and Event Collector.

Viewing Historian Values and Time Stamps in an iFIX Chart

When viewing an iFIX chart, set the interval time to a fine granularity to ensure that you will see Historian values and Time Stamps when you zoom in on the chart.

Importing the Historian Toolbar into iFIX

You must import the Historian toolbar into the iFIX WorkSpace after you have successfully installed Historian.

To import the toolbar:

1. Open the iFIX WorkSpace.
2. Select Toolbars from the WorkSpace menu. The Toolbars dialog box appears.
3. Select WorkSpace from the Owners list.
4. Click the Customize button. The Customize Toolbars dialog box appears.
5. Click the Import button. The Import Toolbars dialog box appears.
6. Select Historian from the Toolbars list.
7. Click the Import button to import the Historian Toolbar.
8. Click the Close button. The Customize Toolbars dialog box closes and the Historian Toolbar appears in the iFIX WorkSpace.

NOTE: *The Configure Historian Servers toolbar in the WorkSpace specifies the location of historical data retrieval for the WorkSpace, not the location of the historical data storage. You can view/retrieve data stored on these listed servers while you select a pen for a chart display. The Configure Historian Servers dialog also determines where HDA programs and historical ODBC retrieve data from, which is always the default server.*

Using the Toolbar Buttons

Use the Change Historian button (left-most button on the toolbar) to switch to Historian mode to browse tags and retrieve data from your Historian Server.

Formatting OPC Tags Containing Special Characters

After selecting an OPC tag in the Expression Builder, you must add single quotes to the pen list in order to handle special characters.

For example:

```
Hist.node1.Data Point.Int2

`Hist.node1.'Data Point.Int2'
```

If a single quote (`) or a backslash (\) is a literal part of the addressing string syntax (e.g. HIST.NODE1.'MIXER'LINE.INT2), it must be preceded by a backslash (\) in order for the character to be passed to the server as part of the address (HIST.NODE1.\'MIXER\'LINE.INT2).

Filtering Tags Using THISNODE with Expression Builder

If you configure an iFIX node to use Local Node Alias and then use for example MIXER as the node name, you can use a filter such as M* to return a list of all tags that start with M including THISNODE. If you use T* as a filter, no tags will be returned, because THISNODE is an alias, not a real node name.

The iFIX Data Collector

Several components of Historian, such as the iFIX Data Collector, work with iFIX. The iFIX Data Collector uses the Easy Data Access (EDA) protocol to retrieve data from a running iFIX system.

The iFIX Install program automatically provides an iFIX node name to the iFIX Data Collector. The default name is iFIXnodename_iFIX. If you browse tags, the Data Collector retrieves every tag with a node name that matches the one you are browsing. Refer to the Historian Data Collector manual for more information on Data Collector tag configuration.

NOTE: *You can install only one iFIX Data Collector per computer.*

The preferred way to start an iFIX Collector is to add the collector to the iFIX System Configuration Utility (SCU) list. The collector then starts automatically whenever you start iFIX.

To add the collector to the SCU list, open the Task Configuration dialog box in iFIX, enter "ihFixCollector.exe" in the Filename field and "runasdos" in the Command Line field, and click the Add button.

IMPORTANT: *Stop the iFIX collector before attempting to modify selected iFIX or FIX database blocks and fields you want to be made available in a browse. You can access the blocks and fields from the Configuration tab of the Collector Maintenance screen.*

Historian and iFIX Chart Objects

The iFIX chart object plots the last recorded value for pens using Historian tags if the data for those tags comes in from a data collector and the collector loses its connection to the data archiver.

Suppose you configure an iFIX chart object to auto-update the historical data. If the data collector loses its connection to the data archiver, the iFIX chart object flatlines at the last recorded value. When the connection between the collector and archiver is reestablished, the chart then shows the correct data for the period in which the collector was not available.

Optionally, you can use a heartbeat to determine when the iFIX Data Collector stops sending data and restart the collector. For more information, refer to the Example: Restarting the iFIX Collector Using a Heartbeat section in chapter 6 of the Historian Data Collectors guide.

Browsing iFIX Tags On Networked iFIX Nodes

It is recommended that you install an iFIX Collector on each node you want to collect data from. You can choose, however, to use the iFIX networking structure to bring tags into your iFIX Collector from multiple iFIX nodes or systems.

To select multiple nodes to browse from modify the Nodes to Browse field in the Configuration Tab of the Collector Maintenance screen. This field displays the mask used to select tags when performing a browse of the collector node. The default is the iFIX SCADA or VIEW (iClient) node name that you installed the collector on. If you want to browse for tags on other iFIX nodes via FIX networking, you can enter the other node name(s) here, separated by commas with no spaces. You must have the iFIX system configured for networking.

For more information, refer to the iFIX Electronic Books on FIX networking.

Creating Historian Charts using Mixed Pens

Historian allows you to put both OPC data source and FIX Tag type pens into your iFIX charts; Classic Historian only allows you to use Fix Tag pens. Note that if you create a mixed pen chart in iFIX Historian Mode and attempt to open the chart in Classic Historian mode, you may not be able to view either pen.

Using the iFIX Expression Editor to search tags

Since iFIX tags have a NODE.TAG.FIELD format, you must enter separate node and tag filters when you use the Expression Editor to search for tags. This is important when you search for non-iFIX tags, such as those generated by a Simulation Collector. For example, if the simulation tags have the format T20.Simulation

00001, T20.Simulation00002, etc., which is different from the iFIX format, use a node filter of * and a tag filter of t2* to return all Simulation tags. An iFIX tag with the name T2.Ramp.F_CV would not be returned in that example because the Tag Name (Ramp) does not contain T2. T2 is the node name.

Searching for Calculation or Server-to-Server tags in the iFIX Expression Editor

You cannot use the Calculation or Server-to-Server Collectors as a search filter in the iFIX Expression Builder. The Calculation or Server-to-Server Collectors do not appear in the Collector Type drop-down list in the iFIX Expression Builder as an option for filtering.

Using the iFIX Integration Toolkit

If you are using the iFIX Integration Toolkit (HDA) with Historian, you must ensure that the HTRDATA directory path location listed in the SCU contains a folder for each node name and a single file with a valid Classic Historian Archive name (for example, "00090300.H24"). If this structure is not in place, all "HdaEnumNodes" calls will fail to return the list of remote nodes. The file does not need to be created by HTC and does not need to contain any historical data. You can create the files using Notepad by saving an empty file as "00090300.H24" including the quotation marks to <Drive:\htrdata\><Remotenodename> where the path matches the HTR data path in the SCU.

GE Intelligent Platforms recommends that all new custom historical data applications be built using the Historian SDK.

Uninstalling Historian if iFIX v2.6 is installed

If iFIX v2.6 is installed, when you uninstall Historian, you should select No if prompted to remove the shared file named SPR32X30.OCX, the Farpoint Spreadsheet v3.0 (a third-party ActiveX control).

If the install removes the SPR32X30.OCX file, the iFIX WorkSpace reports a VBA compile error the next time you open the iFIX WorkSpace.

If you receive the compile error when you open the iFIX WorkSpace, run the following command from the iFIX base path:

```
regsvr32 SPR32X30.OCX
```

This command re-registers the Farpoint Spreadsheet.

Using v7.x Drivers with Historian

Consult the following topics for using the iFIX v7.x drivers with Historian

- Using Autocreate
- Using the Latched Data feature
- Running iFIX 7.x Drivers as OPC Servers
- Running iFIX 7.x Drivers as a service with Automatic Startup

Using Autocreate

iFIX 7.X drivers have an AutoCreate feature that automatically generates datablocks if an iFIX Database or an OPC Collector requests them. If you have enabled AutoCreate in an Intellution 7.X driver that you are using with Historian, any datablock deleted from a group will be recreated by the next collector request. To stop the recreation, disable AutoCreate for the driver. You cannot specify only iFIX AutoCreate.

Using the Latched Data feature

iFIX 7.X drivers running as OPC Servers have a latched data feature. If you select this feature, the driver continues to display the last known good value, even when a connection to the process hardware is broken. The Historian OPC Collector considers the latched values as bad data and does not collect the values.

Running iFIX 7.x Drivers as OPC Servers

Current versions of iFIX 7.X drivers can run as OPC Servers. If you are running 7.X drivers as OPC Servers, you must either run the 7.X driver on a computer with iFIX installed or install the new hardware key.

Running iFIX 7.x Drivers as a service with Automatic Startup

The following procedure details the steps needed to set up your iFIX 7.X driver to run as a service with automatic startup. The procedure describes a specific ABR driver setup which requires RSLinx; however, you can also use the steps to configure your other 7.X drivers by substituting the driver name and other specific driver information. If your driver requires a third party software, such as RSLinx, ensure that it is configured properly as a service before moving on to step 2.

To set a collector to run as a service with the ABR driver:

1. Install and configure Rockwell Software's RSLinx.

2. Install an ABR OPC Server.
3. Create an ABR Configuration, save it, and configure it for auto start.
4. Install and configure your OPC Collector:
    a. Install an OPC collector. The Historian install prompts you for a Prog ID and a name.
    b. Enter Intellution.ABROPC.
    c. Choose not to restart your system.
5. Configure DCOM defaults.

    NOTE: *You should only need to configure DCOM on your Windows computer once.*

    a. Select Run from the Start menu and enter DCOMCNFG. The Distributed COM Configuration Properties dialog box appears.
    b. Select the Default Security tab.
    c. Click the Edit Default button in the Default Access Permissions section.
    d. Click the Add button to add System and Interactive Groups (if not present).
    e. Click OK to return to the Distributed COM Configuration Properties dialog box.
    f. Click the Edit the Default button in the Default Launch Permissions section.
    g. Click the Add button to add System and Interactive Groups (if not present).
    h. Click OK to return to the Distributed COM Configuration Properties dialog box.
    i. Click Edit the Default button in the Default Configuration Permissions section.
    j. Click the Add button to add System and Interactive Groups (if not present).
    k. Click Apply and OK to close the DCOM configuration utility.
6. Register Intellution OPC Server to run as a service:
    a. Ensure that the Power Tool and all clients are shut down.
    b. At the run prompt, enter the following:

        ABRdrv REGSERVICE

        Note that this text is case sensitive.

    a. Verify that the ABR OPC Server appears in the Services dialog box. If it does not, you may have entered it incorrectly. Ensure that all client applications to the driver, including the Power Tool, are closed and the Services Dialog is closed. If all client applications are closed, try entering the string again.
7. Start the Server manually through the Services Dialog in the Control Panel.

8. Start the Collector manually through the Control Panel.
9. Log into the Historian Administrator and add all of the tags from the collector.
10. Open the Run prompt from the Start Menu.
11. Enter Regedt32 in the Open field and set the following dependencies:

    Set the Dependency of the iHOPCCollector on the OPCServer:

    a. Locate the iHOPCCollector folder. This folder is typically located in the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\iHOPCCollector path.

    b. Add a value to the iHOPCCollector registry key:

        I. Select Add a Value from the Edit menu.

        II. Enter the following exactly in the Value field:

            DependOnService

        III. Select REG_MULTI_SZ as the data type.

        IV. Click OK. A dialog box appears prompting you to enter the value.

        V. Enter ABRdrv.

        VI. Click OK.

    c. Set Dependency of OPC server on its 3rd party API:

        NOTE: *This dependency only applies to the ABR and other drivers which require a 3rd party API. For all other 7.X drivers, only set the iHOPCCollector dependency.*

        I. Locate the ABRdrv folder. This folder is typically located in the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ABRdrv path.

        II. Add RSLinx to DependOnService:REG_MULTI_SZ value.

12. Open Services in the Control Panel.
13. Select and set the ABRdrv and iHOPCCollector Startup to automatic.
14. Configure RSLINX to run as a Service:
    a. Select Options from the View menu.
    b. Select the Service Tab.
    c. Select the Run as a Service check box.
15. Restart your computer.
16. Verify that all services started, and that data is being collected.

Troubleshooting iFIX and Historian

Consult the following topics for troubleshooting iFIX and Historian.

- Running iFIX as a service with Workspace listed in the SCU Task List
- iFIX Workspace delay when remote session is lost
- Starting iFIX when a remote Historian session is unavailable
- Accessing Mission Control when a remote Historian session is lost
- Using the iFIX V2.6 chart with Historian domain security enabled
- Accessing tags in the iFIX chart after setting OPC Collector to "Made After Restart"
- Collecting data in an iFIX chart with Time Assigned By Source

Running iFIX as a service with Workspace listed in the SCU Task List

Prior to iFIX 5.1, if you have configured iFIX to run as a service, you should not have WORKSPACE.EXE listed as a configured task in the Task Configuration dialog box of the SCU. If WORKSPACE.EXE is listed as a configured task, it may lead to unpredictable results. For example, if you are also running Historian, no servers will appear in the Server Name field of the Configure the Historian Server dialog box and you will not be able to browse Historian tags in the iFIX Expression Editor.

To rectify this, remove WORKSPACE.EXE from the list of configured tasks in the SCU.

iFIX Workspace delay when remote session is lost

If the connection between iFIX and a remote Historian session is lost, you may experience a 90 second delay in the iFIX Workspace Configuration environment, chart, or Expression Builder when accessing a pen associated with that Historian session.

In the Run Time Environment, all pens in a chart disappear for 90 seconds when the session to a remote Historian session is lost, even if they are associated with a local Historian server.

Starting iFIX when a remote Historian session is unavailable

If you are using Historian with iFIX, the iFIX Workspace attempts to connect to the Historian Server when it starts up. If a remote Historian server is unavailable, it may take one minute or longer for iFIX Workspace to display for each unavailable server.

Accessing Mission Control when a remote Historian session is lost

If a remote Historian session is lost while you are accessing `the HTC tab of Mission Control in the iFIX Workspace, the H tab may blank out for a minute or longer.

Using the iFIX V2.6 chart with Historian domain security enabled

If you have enabled Historian Domain Security in the Historian Administrator, you will need to download the latest iFIX v2.6 SIM to use the iFIX Chart. For more information on iFIX SIMs, refer to http://support.ge-ip.com/downloads/sims/ or contact your local sales representative.

Accessing tags in the iFIX chart after setting OPC Collector to "Made After Restart"

If you add tags in the Historian Administrator to a Server from an OPC Collector that has Configuration Changes set to Made After Collector Restart, you will be able to see those tags in the iFIX Expression Builder. You can add them to a chart, for example, but they have no collected data until you manually stop and restart the OPC Collector.

Collecting data in an iFIX chart with Time Assigned By Source

If you are retrieving data in an iFIX Chart from an Historian Server, have set the Time Assigned by field to Source, and have collectors running behind the Server time, the chart will display a flatline up to the current time of the local machine.

NOTE: *You must set Time Assigned by field to Source if you have unsolicited tags getting data from an OPC Collector.*

Synchronizing the time on iFIX SCADA Servers and View Clients

To ensure that acknowledgements are not lost or attributed to the wrong alarm, synchronize the clocks on SCADA servers and iFIX View Client machines. If the clocks are not synchronized, alarms generated on the SCADA nodes and acknowledged on the iFIX View Client nodes could have significantly different timestamps. You can synchronize the clocks using the NET TIME command. Refer to the Windows Help system for more information.

Startup Procedure Overview

To install and start up Historian in the shortest possible time:

1. Define your system architecture.

   Decide what collectors to install on which nodes, what computers to designate as the Historian Server and the Historian Administrators, whether or not they will be web-based, and how much memory and disk space you can assign to buffers and archives. Record the computer names of each node.

2. Ensure that iFIX and other data sources are installed.
3. Set up your Historian environment. (Refer to Chapter 2.)
4. At the server node, power off the computer, plug the Hardware Key into the parallel port or USB port, and restart. (Refer to Chapter 2.)

   IMPORTANT: *For USB keys, skip step 5, and proceed to install the Historian product software. After installing the Historian, software then you can plug in the key.*

5. At the server node, insert the Historian DVD and select Historian Install. Respond to prompts, selecting Historian Server for installation. If you want other items installed on the Server, select them at the same time as the Historian Server.

   NOTE: *If you forget to add a component and re-run the install do not unselect previously installed components as they will be uninstalled.*

7. Install collectors where needed.

   - **iFIX** &endash; Select the Historian iFIX Collector to collect data and/or the iFIX AE Collector to collect alarms and events. When prompted, type in the name of the Historian server as the destination for archived data.
   - **OPC Alarms & Events** &endash; To collect data from an OPC AE server select the OPC AE collector and when prompted select the name of the OPC AE server.
   - **OPC Data** &endash; To collect data from an OPC v1.0/2.0 server select the OPC Data collector and when prompted select the OPC data collector from the list provided.
   - **Calculation** &endash; To install a calculation collector select it from the list of options and when prompted type in the name of the Historian server as the destination for the calculated values
   - **Server-to-Server** &endash; Select the Server-to-Server collector to collect data from one Historian server (”r;Source”) and store it on another (”r;Destination”). When prompted, type in the name of both the source and destination Historians.
   - **Server-to-Server Distributor** - Select the Server-to-Server Distributor to configure tags at

the source archiver and send the tags to a destination archiver. When prompted, type in the name of both the source and destination Historians.

- **OSI PI** &endash; Select the OSI PI collector to collect data from an OSI PI node and store it in the Historian. Select the OSI PI Distributor to collect data from the Historian server and store it on an OSI PI node. When prompted, type in the name of the OSI PI and Historian servers

8. Restart your computer if prompted to.

   If your collector services are not configured for automatic start up, manually start them.

9. At the non-web-based Administration clients, start the Administrator from the Historian Startup Group. When the Historian Administrator's main screen appears, you are ready to set up archives, collectors, and tags in the Data Store Maintenance, Collector Maintenance, and Tag Maintenance screens. Refer to the Using the Historian Administrator manual for details.

   NOTE: *Collectors will not appear in the Historian Administrator until they are started.*

Contact GE Intelligent Platforms

If you purchased this product through an Authorized Channel Partner, please contact the seller directly.

General Contact Information

Online technical support & GlobalCare: www.ge-ip.com/support

Comments about our manuals and online Help: doc@ge.com

Additional information: www.ge-ip.com

Solution Provider: solutionprovider.ip@ge.com

Authorization: authorization.ip@ge.com

Technical Support

If you have technical problems that cannot be resolved with the information in this guide, please contact us by telephone or e-mail, or on the web at www.ge-ip.com/support.

Americas

Online technical support: www.ge-ip.com/support

Telephone: 1-800-433-2682

International Americas direct dial: 1-780-420-2010 (if toll free 800 option is unavailable)

Technical Support e-mail: support.ip@ge.com

Customer Care e-mail: customercare.ip@ge.com

Inside Sales: insidesales.ip@ge.com

Primary language of support: English

Europe, Middle East, and Africa

Online technical support: www.ge-ip.com/support

Telephone: +800 1-433-2682

EMEA direct dial: +1 780-401-7717 (if the toll free 800 option is not available in your country, or if dialing from a mobile telephone)

Technical Support e-mail: support.emea.ip@ge.com

Customer Care e-mail: customercare.emea.ip@ge.com

Inside Sales: insidesales.emea.ip@ge.com

Primary language(s) of support: English, French, German, Italian, Czech, Spanish

Asia Pacific

Online technical support & GlobalCare: www.ge-ip.com/support

Telephone: +86-400-820-8208,

+86-21-3217-4826 (India, Indonesia, and Pakistan)

Technical Support e-mail: support.cn.ip@ge.com (China)

support.jp.ip@ge.com (Japan)

support.in.ip@ge.com (other Asian locales)

Customer Care e-mail: customercare.apo.ip@ge.com

customercare.cn.ip@ge.com (China)